

Perspektiven:

Cyber Resilience für die Bahn von morgen – oder volle Fahrt in die Krise?

WAVESTONE

INHALT

Vorwort 3

Hybride Bedrohung im KRITIS-Sektor Transport und Verkehr:
Warum Resilienz zur eigentlichen Führungsaufgabe wird 4

NIS2 im Bahnsektor:
Pflichten entlang der Bahnleistungen umsetzen 10

IT/OT-Konvergenz im Bahnsektor:
Die Sicherheit entscheidet sich an den Übergängen 22

OT-Security in der Bahn:
„Wir brauchen weniger Know-how und mehr Do-how“ 28

Assetmanagement im Bahnsektor:
Die Grundlage jeder Sicherheitsentscheidung 32

Cyber Resilienz in der Lieferkette:
NIS2 und CRA verändern die Zusammenarbeit im Bahnsektor 40

KI-gestütztes Security Monitoring im Bahnsektor:
Erst das Fundament, dann die Automatisierung 48

BCM auf die Schiene bringen:
Pläne, die im Ereignisfall funktionieren 54

Krisenmanagement im Bahnsektor:
Von gemeinsamen Begriffen zur Handlungsfähigkeit 62

Workforce Readiness im Bahnsektor:
Der blinde Fleck der Operational Resilience 68

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

VORWORT

Im Februar 2026 waren Auskunft und Buchung der Deutschen Bahn durch einen DDoS-Angriff wiederholt in einer Größenordnung gestört, die selbst das BSI als nicht alltäglich einordnete. Ein Einzelfall ist das nicht: Sabotage an der Strecke, Cyberangriffe und Desinformation treten im Bahnsektor zunehmend und gleichzeitig auf. Sie richten sich gegen eine Infrastruktur, die für die Versorgung ebenso gebraucht wird wie für die Verteidigung.

Hinzu kommen neue Anforderungen. Seit Dezember 2025 gilt das neue BSI-Gesetz zur Umsetzung von NIS2, das Geschäftsleitungen direkt in die Pflicht nimmt. Das KRITIS-Dachgesetz verlangt seit März 2026 zusätzlich Maßnahmen zur physischen Resilienz. Der Cyber Resilience Act richtet sich an die Hersteller digitaler Produkte; erste Meldepflichten gelten hier seit September 2026. Außerdem entstehen mit jedem Digitalisierungsprojekt weitere Verbindungen zwischen betrieblicher OT und Unternehmens-IT, die auch im Ernstfall beherrschbar bleiben müssen.

Diese Publikation zeigt in zehn Beiträgen, wie Bahnunternehmen ihre Cyber Resilienz gezielt stärken können. Die Themen reichen von hybriden Bedrohungen, NIS2, IT/OT-Konvergenz, OT-Security und Assetmanagement über die Lieferkette und KI im Security Monitoring bis zu Business Continuity, Krisenmanagement und der Frage, ob im Ernstfall genügend qualifiziertes Personal verfügbar ist. Maßstab ist dabei immer der Bahnbetrieb: Läuft der Zugverkehr auch unter Störbedingungen kontrolliert weiter?

Die Beiträge beruhen auf Gesprächen mit Praktikern aus dem Bahnsektor und angrenzenden Branchen. Für ihre offenen Einschätzungen danken wir Uwe Füller (DSV), Ulrich Zackor (DB InfraGO), Martin Heiderich (Hitachi Rail), Tim Neubert (Rheinbahn AG), Thomas Theisejans (Deutsche Bahn AG), Nico Gramenz (takeKONTROL) sowie weiteren, nicht namentlich genannten Gesprächspartnern. Der Titel stellt bewusst eine zugespitzte Frage. Die Beiträge geben darauf eine gemeinsame Antwort: Resilienz entsteht an den Schnittstellen. Es kommt darauf an, wie gut Security, Business Continuity, Krisenmanagement, IT und OT-Security, Lieferanten und Personal zusammenwirken. Wo diese Bereiche getrennt geplant und gesteuert werden, bleiben im Ernstfall Lücken. Wir freuen uns auf den Austausch darüber, wo Bahnunternehmen heute stehen und welche Schritte jetzt folgen sollten.



Astrid Blechschmidt
Partner, Reisen, Transport & Logistik

Hybride Bedrohung im KRITIS-Sektor Transport und Verkehr: Warum Resilienz zur eigentlichen Führungsaufgabe wird

Cybersecurity im Bahnsektor wird häufig als technisches Thema diskutiert. Das greift zu kurz: Sabotage an Bahnanlagen, Angriffe auf den Zugfunk und Überlastangriffe auf Buchungsportale zeigen, dass physische, digitale und gesellschaftliche Angriffsformen gleichzeitig wirken. Dieser Beitrag ordnet die hybride Bedrohungslage ein und bildet den Rahmen für die folgenden Beiträge.

*Grundlage ist ein Gespräch mit **Uwe Füller**, Director IT Crisis Management & Resilience bei DSV.*
*Autor: **Martin Wölfel**, Senior Manager, Wavestone*

KEY TAKEAWAYS

- **Dauerhaft hybride Lage:** Sabotage, Cyberangriffe und Desinformation treffen den Bahnsektor nicht mehr als Einzelfälle. Sie überlagern sich und gehören zum Betriebsalltag.
- **Zwei Treiber:** Geopolitische Spannungen und KI-gestützte Angriffe verstärken sich gegenseitig.
- **Besonders exponiert:** Verkehr, Logistik und Bahn sind versorgungs- und verteidigungsrelevant und damit zugleich ein Hebel, um die Gesellschaft zu destabilisieren.
- **Schwächstes Glied:** Die größten Lücken liegen häufig bei Lieferanten, Dienstleistern und regionalen Standorten.
- **Resilienz als Führungsaufgabe:** Weitere Einzelmaßnahmen helfen wenig. Wirksam wird der Schutz erst, wenn Security, Business Continuity Management (BCM), Krisenmanagement, IT und OT gemeinsam gesteuert werden.

Die Bedrohungslage ist dauerhaft hybrid

Die Zahl der Angriffe wächst, vor allem aber haben sich ihre Qualität und Gleichzeitigkeit verändert.

Physische, digitale und gesellschaftliche Angriffsformen überlagern sich zunehmend. Beispiele sind der Ausfall des GSM-R-Zugfunks der Deutschen Bahn im Oktober 2022, der Sprengstoffanschlag auf die Bahnstrecke Warschau–Lublin im November 2025, über die auch Lieferungen in die Ukraine laufen, und die DDoS-Angriffe auf Auskunft und Buchung der Deutschen Bahn im Februar 2026. Hinzu kommen koordinierte Kabeldiebstähle mit weitreichender Betriebswirkung. Alle diese Angriffe bleiben unterhalb der Schwelle eines offenen Konflikts. Füller beschreibt die Lage so: *„Wir leben in einer VUKA-Welt, und die aktuelle Konvergenz aus geopolitischer Spannungslage und technologischer Beschleunigung erzeugt einen Druck, den wir in dieser Form bisher nicht kannten.“* Für den Betrieb bedeutet das eine grundsätzliche Verschiebung: Bedrohungen sind nicht mehr situativ, sondern strukturell. Wer weiterhin nur einzelne Szenarien plant, unterschätzt sowohl die Gleichzeitigkeit als auch die Wirkungstiefe.

Zwei Treiber verstärken die Lage: Geopolitik und Technologie

Geopolitische Spannungen und KI verschärfen die hybride Bedrohung. Und beide verstärken sich gegenseitig.

Der erste Treiber ist geopolitisch. Kritische Infrastrukturen sind zum Instrument staatlicher und staatsnaher Akteure geworden. Verkehrsinfrastruktur eignet sich dafür besonders. Sie versorgt Bevölkerung und Wirtschaft, ist für Truppentransporte im Bündnis unverzichtbar, und jeder Ausfall ist sofort öffentlich sichtbar. *„Auf der einen Seite haben wir eine geopolitische und ökonomische Spannungslage, auf der anderen einen Technologiestrang, der klar durch Künstliche Intelligenz getrieben ist. Beides zusammen verstärkt das Gesamtrisiko massiv“*, so Füller.

Der zweite Treiber ist technologisch. Mit KI lassen sich Angriffe schneller und in größerer Zahl durchführen. Schwachstellen werden automatisiert und massenhaft ausgenutzt, Schadsoftware passt sich selbst an und den Verteidigern bleibt immer weniger Zeit zu reagieren. Hinzu kommt maschinell erzeugte Desinformation, die die öffentliche Wirkung eines Angriffs verstärkt. Füller spricht in diesem Zusammenhang bereits vom *„Kampf der Maschinen“*: *„Angreifer skalieren über KI, und Verteidiger müssen genauso automatisieren, um überhaupt reagieren zu können.“* Die weiteren Möglichkeiten und Grenzen dieser Entwicklung greift der Beitrag **„KI-gestütztes Security Monitoring im Bahnsektor: Erst das Fundament, dann die Automatisierung“** ↗ auf.

Warum Bahn und Verkehr besonders exponiert sind

Verkehrsinfrastruktur ist ein strategisches Ziel: Sie sichert Versorgung und Verteidigung, und jeder Ausfall ist sofort öffentlich spürbar.

Der Bahnsektor ist das Rückgrat der Personen- und Güterlogistik und damit Voraussetzung wirtschaftlicher Funktionsfähigkeit. Er ist zugleich verteidigungsrelevant: Ohne funktionierende Schienen, Straßen, Häfen und Flughäfen ist kein Bündnisraum handlungsfähig. Hinzu kommt die gesellschaftliche Wirkung. Fällt der Schienenverkehr über einen längeren Zeitraum aus, spüren das Pendler und Wirtschaft unmittelbar, und die Politik gerät unter Druck. Diese Sichtbarkeit macht den Bahnsektor zu einem attraktiven Ziel für Akteure, die Destabilisierung beabsichtigen. Bahnunternehmen müssen sich deshalb auf Angriffe einstellen, die digitale, physische und narrative Mittel kombinieren, etwa eine Sabotage an der Strecke, die von einer Desinformationskampagne in sozialen Medien begleitet wird.

Das schwächste Glied liegt selten im eigenen Unternehmen

Hybride Angriffe zielen auf die gesamte Wertschöpfungskette. Besonders verwundbar sind die Stellen, an denen Zuständigkeiten enden.

Viele Bahnunternehmen haben ihre eigene Sicherheitsarchitektur spürbar gestärkt. Das reicht nicht aus, wenn Lieferanten, Dienstleister oder regionale Standorte ein niedrigeres Schutzniveau aufweisen. *„Die Frage ist doch, wo das schwächste Glied liegt – und das muss nicht das Unternehmen selbst sein. Bricht es in der Lieferkette, ist der Impact trotzdem da“*, stellt Füller fest. Der Beitrag **„Cyber Resilienz in der Lieferkette“** ↗ vertieft, wie Resilienz entlang der Lieferkette methodisch und vertraglich verankert wird. Für global agierende Verkehrs- und Logistikunternehmen kommt eine regionale Dimension hinzu: Globale Rahmenwerke müssen durch lokale Handlungsfähigkeit ergänzt werden. Auch hier ist Füller eindeutig: *„Globale Frameworks müssen downstream implementiert und in den Regionen trainiert werden, damit auf regionaler Ebene tatsächlich Handlungsfähigkeit entsteht.“*

Resilienz verbindet die Sicherheitsdomänen

Hybride Bedrohungen lassen sich nicht vollständig verhindern. Resilient ist, wer Angriffe verkraftet, den Betrieb aufrechterhält und schnell wieder in einen kontrollierten Zustand zurückkehrt.

Eine weitere Sicherheitsdisziplin hilft gegen hybride Bedrohungen wenig. Es geht darum, die bestehenden Disziplinen zu verbinden. Drei Handlungsfelder sind dabei zentral:

- **Continuity** sichert die Fortführung kritischer Leistungen. Wie das im Bahnsektor operativ verankert wird, beschreibt der Beitrag **„BCM auf die Schiene bringen: Pläne, die im Ereignisfall funktionieren“**↗.
- **Protection** verbindet Informationssicherheit mit physischer Sicherung, Corporate Security und OT-Schutz. Der Beitrag **„IT/OT-Konvergenz im Bahnbetrieb“**↗ und der Beitrag **„Asset Management über IT und OT hinweg“**↗ setzen hier vertiefend an. Wie OT-Security in der Praxis aussieht, schildert Ulrich Zackor, Head of OT-Security bei DB InfraGO, im Interview **„OT-Security in der Bahn“**↗.
- **Reaktion und Führung** entscheiden im Ereignisfall über das Ausmaß des Schadens. Ohne eingeübtes Krisen- und Notfallmanagement bleiben Continuity und Protection wirkungslos. Der Beitrag **„Krisenmanagement im Bahnsektor: Von gemeinsamen Begriffen zur Handlungsfähigkeit“**↗ adressiert diesen Aspekt.

Übergreifend wird der regulatorische Rahmen durch NIS2 sowie das KRITIS-Dachgesetz geprägt, das die CER-Richtlinie in deutsches Recht umsetzt. Der Beitrag **„NIS2 im Bahnsektor: Pflichten entlang der Bahnleistungen umsetzen“**↗ ordnet diese Anforderungen ein. Füller fasst den entscheidenden Schritt so zusammen: *„Am Ende brauchst du ein Forward-Looking Risk Management. Ein Verständnis dafür, was auf dich zukommt, bevor es eintritt – getragen von Menschen mit dem richtigen Mindset, die Brücken zwischen den Managementdisziplinen bauen.“* Dass Resilienz letztlich von Menschen getragen wird, zeigt auch der Beitrag **„Workforce Readiness im Bahnsektor: Der blinde Fleck der Operational Resilience“**↗. Er beschreibt, wie Bahnunternehmen sicherstellen, dass genügend qualifizierte Beschäftigte im Ernstfall tatsächlich verfügbar sind.

Operative Resilienz setzt voraus, dass Security, BCM, Krisenmanagement, Lieferkettensteuerung, IT und OT auf gemeinsame Ziele ausgerichtet sind. Organisatorische Resilienz braucht zusätzlich eine gemeinsame Führungs- und Entscheidungskultur.

Was Bahnunternehmen jetzt konkret tun sollten

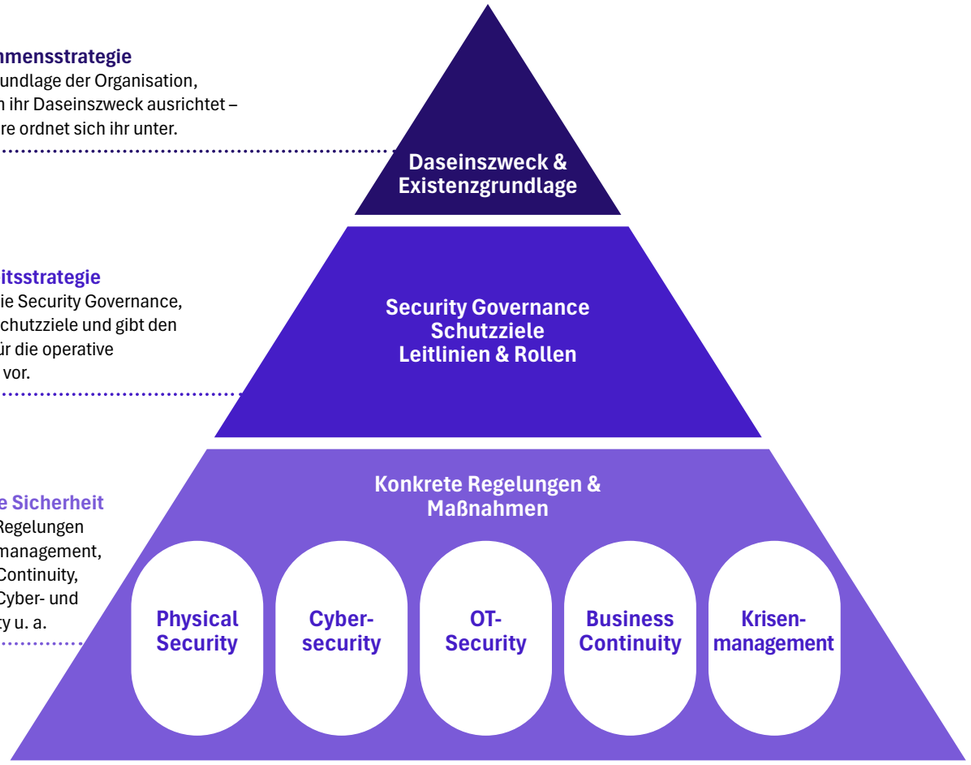
Aus der hybriden Bedrohungslage ergeben sich drei Schritte:

1. **Bedrohungsbild aktualisieren und in die Führung überführen.** Hybride Szenarien gehören in Vorstand und Aufsichtsgremien, nicht nur in Sicherheitsberichte.

2. **Silos zwischen Security, BCM, Krisenmanagement, IT und OT auflösen.** Ein gemeinsames Zielsystem und geübte Schnittstellen wirken stärker als weitere Einzelmaßnahmen.

3. **Resilienz entlang der Lieferkette und in den Regionen aufbauen.** Globale Rahmenwerke müssen lokal handlungsfähig gemacht werden.

Hybride Bedrohungen werden den Bahnbetrieb dauerhaft prägen. Die folgenden Beiträge zeigen, wie Bahnunternehmen in den einzelnen Bereichen vorgehen können, von der Regulierung über die OT-Security bis zum Krisenmanagement. Wavestone unterstützt Bahnunternehmen dabei, diese Bereiche zu einer gemeinsamen Resilienzstrategie zusammenzuführen.



NIS2 im Bahnsektor: Pflichten entlang der Bahnleistungen umsetzen

Der Bahnbetrieb basiert auf einer eng gekoppelten Wertschöpfungskette: Betriebsführung, Leit- und Sicherungstechnik, Fahrzeuge, Energieversorgung, Kommunikationsnetze, Reisendeninformation und externe Partner greifen unmittelbar ineinander. Mit dem Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 2. Dezember 2025 wurden die europäischen Vorgaben insbesondere durch eine Neufassung des BSI-Gesetzes (BSIG) in deutsches Recht überführt. Das neue BSI-Gesetz gilt seit dem 6. Dezember 2025. Bahnunternehmen müssen seitdem ihre Betroffenheit und den relevanten Scope nachvollziehbar bestimmen, Cyberrisiken an den Auswirkungen auf Verkehrs- und Infrastrukturleistungen ausrichten und ihre Handlungsfähigkeit bei Sicherheitsvorfällen nachweisbar sicherstellen.

*Autoren: **Jonathan Schläger**, Partner, Wavestone*
***Marc-André Ohk**, Managing Consultant, Wavestone*



KEY TAKEAWAYS

- **Betroffenheit je Einrichtung prüfen:** Der Schienenverkehr ist ausdrücklich erfasst. Eisenbahninfrastrukturunternehmen, Eisenbahnverkehrsunternehmen und Betreiber von Serviceeinrichtungen müssen ihre **Betroffenheit je Einrichtung prüfen**; Betreiber kritischer Anlagen gelten als besonders wichtige Einrichtungen. (§ 28 Abs. 1 und 2 BSIG; Anlage 1 Nr. 2.2 BSIG)
- **Betriebliche Systeme einbeziehen:** Der Scope muss über die klassische Unternehmens-IT hinausreichen. Für die Bahnleistungen genutzte Stellwerks-, Leit-, Fernwirk-, Fahrzeug-, Werkstatt- und Kommunikationssysteme sind ebenso zu berücksichtigen wie Abhängigkeiten von Standorten, betrieblichen Rollen und externen Partnern. (§ 30 Abs. 1 BSIG)
- **Kompensierende Maßnahmen für die OT:** Gewachsene OT-Landschaften erschweren die Umsetzung: lange Lebenszyklen, begrenzte Wartungsfenster, Safety- und Zulassungsanforderungen sowie Herstellerabhängigkeiten schränken klassische IT-Maßnahmen ein. Erforderlich sind deshalb risikobasierte Schutzkonzepte und gegebenenfalls kompensierende Maßnahmen, etwa Segmentierung, kontrollierte Fernwartung und verstärkte Überwachung.
- **Verantwortung der Geschäftsleitung:** Geschäftsleitungen müssen Risikomanagementmaßnahmen umsetzen, deren Umsetzung überwachen und regelmäßig an Schulungen teilnehmen. Informationssicherheitsverantwortliche schaffen dafür eine Entscheidungsgrundlage zu Risiken, Maßnahmen, Wirksamkeit und Restrisiken. Bei Verstößen drohen dem Unternehmen erhebliche Bußgelder. Geschäftsleitungen haften bei schuldhaften Pflichtverletzungen gegenüber der eigenen Einrichtung. (§§ 38 und 65 BSIG)
- **Gestufte Meldefristen:** Erhebliche Sicherheitsvorfälle lösen gestufte Meldepflichten aus: eine frühe Erstmeldung binnen 24 Stunden, eine Vorfallsmeldung binnen 72 Stunden und grundsätzlich eine Abschlussmeldung spätestens einen Monat nach der 72-Stunden-Meldung. (§ 32 Abs. 1 und 2 BSIG)
- **Mehrwert durch Integration:** Einen Nutzen über die Compliance hinaus bringt NIS2, wenn die Anforderungen in bestehende ISMS-, BCM-, Engineering-, Safety- und Lieferantenprozesse integriert und anhand realistischer Bahnszenarien erprobt werden.

Cyber Resilienz ist Managementaufgabe

NIS2 nimmt die Geschäftsleitung direkt in die Pflicht – mit Folgen für Überwachung, Schulung und Haftung.

Weil die Bereiche des Bahnbetriebs eng gekoppelt sind, bleiben Sicherheitsvorfälle selten auf ein einzelnes System begrenzt: Der Ausfall einer Dispositionsplattform kann Zugreihenfolgen und Störungssteuerung beeinträchtigen, eine Störung der Reisendeninformation kann Anzeigen, Durchsagen und digitale Kanäle zugleich treffen, und Einschränkungen im Werkstatt- oder Flottenmanagement können die Fahrzeugverfügbarkeit reduzieren. Cyberrisiken sind damit immer auch Betriebs-, Leistungs- und Unternehmensrisiken.

Der Gesetzgeber weist der Geschäftsleitung deshalb eine unmittelbare Rolle zu. Sie muss die erforderlichen Risikomanagementmaßnahmen umsetzen, deren Umsetzung überwachen und regelmäßig an Schulungen teilnehmen. Für Informationssicherheitsverantwortliche folgt daraus die Aufgabe, Risiken, Maßnahmenstatus, Wirksamkeit und Restrisiken so aufzubereiten, dass die Geschäftsleitung fundierte Entscheidungen treffen und ihre Überwachungsverantwortung dokumentiert wahrnehmen kann. (§ 38 Abs. 1 und 3 BSIG)

Diese Verantwortung ist auch haftungsrechtlich relevant. Verletzt ein Mitglied der Geschäftsleitung seine Umsetzungs- oder Überwachungspflichten schuldhaft und entsteht der Einrichtung dadurch ein Schaden, kann eine Haftung nach den anwendbaren gesellschaftsrechtlichen Regeln entstehen. Verstöße des Unternehmens gegen Risiko-, Dokumentations- oder Meldepflichten können zudem erhebliche Bußgelder auslösen. (§ 38 Abs. 2 BSIG; § 65 Abs. 2 und Abs. 5 bis 8 BSIG)

Welche Pflichten für Bahnunternehmen gelten

Die Pflichten reichen von der Registrierung über Risikomanagement und Meldewege bis zur Verantwortung der Geschäftsleitung und greifen ineinander.

Beherrschbar werden diese Pflichten, wenn Bahnunternehmen sie auf ihre kritischen Bahnleistungen übertragen und für jede Pflicht Verantwortliche, Prozesse und überprüfbare Ergebnisse festlegen. Der konkrete Pflichtenumfang richtet sich nach der Einstufung der jeweiligen Einrichtung und danach, ob sie zugleich Betreiber kritischer Anlagen ist.

Betroffenheit, Einstufung und Registrierung klären

Eisenbahninfrastrukturunternehmen, Eisenbahnverkehrsunternehmen und Betreiber von Serviceeinrichtungen müssen prüfen, ob sie als wichtige oder besonders wichtige Einrichtung gelten. Maßgeblich sind Tätigkeit, Größenmerkmale und eine mögliche Eigenschaft als Betreiber kritischer Anlagen. Bei der Registrierung sind zwei Verfahren zu unterscheiden: Besonders wichtige und wichtige Einrichtungen registrieren sich grundsätzlich spätestens drei Monate nach Eintritt der Betroffenheit nach § 33 Abs. 1 BSIG. Änderungen sind unverzüglich, spätestens innerhalb von zwei Wochen nach Kenntnis, zu aktualisieren. Die Registrierung kritischer Anlagen erfolgt nach § 33 Abs. 2 BSIG in Verbindung mit § 8 KRITIS-Dachgesetz. Bahnunternehmen sollten deshalb sowohl die Einstufung ihrer juristischen Einheiten als auch eine mögliche Kritikalität einzelner Anlagen prüfen. (§ 28 BSIG; Anlage 1 Nr. 2.2 BSIG; § 33 Abs. 1, 2 und 5 BSIG; § 8 KRITIS-Dachgesetz)

Im Bahnsektor ist diese Analyse besonders anspruchsvoll. Infrastruktur, Verkehrsleistungen und Serviceeinrichtungen werden oft von unterschiedlichen Gesellschaften erbracht, während Leitstellen, Betriebsfunk, Rechenzentren, Kommunikationsnetze sowie Werkstatt- und Fahrzeugmanagementsysteme konzernweit oder standortübergreifend genutzt werden. Wem ein System gehört, wer es betreibt und wer dafür verantwortlich ist, kann auseinanderfallen. Welche Gesellschaft regulatorisch betroffen ist, lässt sich deshalb nicht immer an der Organisationsstruktur ablesen.

Hinzu kommt, dass sich der Scope aus den tatsächlich erbrachten Bahnleistungen und ihren Abhängigkeiten ergibt, nicht aus einzelnen Assets. So kann ein digitales Stellwerk, eine zentrale Leitstelle oder ein System der Bahnstromversorgung für mehrere Strecken, Regionen oder Gesellschaften gleichzeitig eingesetzt werden. Auch Fahrzeug-IT, Werkstattsteuerung oder Reisendeninformationssysteme dienen häufig mehreren Verkehrsleistungen. Schwierig ist deshalb vor allem, die gesetzlichen Anforderungen über die organisatorischen Einheiten hinaus auf die dahinterliegenden betrieblichen Leistungsbeziehungen, technischen Schnittstellen und externen Abhängigkeiten anzuwenden.

Für bisherige KRITIS-Betreiber liegt der Aufwand vor allem im erweiterten Scope. Viele kleinere Eisenbahnverkehrsunternehmen und Betreiber von Serviceeinrichtungen sind dagegen erstmals erfasst. Sie beginnen bei den Grundlagen: Registrierung, Scope-Bestimmung, Asset-Inventar und Meldeprozess.

Risikomanagement an den Bahnleistungen ausrichten

Betroffene Einrichtungen müssen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen umsetzen und deren Einhaltung dokumentieren. Im Bahnkontext betrifft dies unter anderem Stellwerks- und Leitsysteme, Betriebsfunk, Fahrzeug-IT, Flotten- und Umlaufplanung, Werkstattsteuerung, Ticketing und Reisendeninformation. Zu den gesetzlichen Maßnahmenbereichen gehören Risikoanalyse, Vorfallbewältigung, Betriebsfortführung, Lieferkettensicherheit, sichere Beschaffung und Wartung, Wirksamkeitsbewertung, Schulung, Kryptografie, Zugriffskontrolle, Assetmanagement, Multi-Faktor-Authentifizierung und sichere Kommunikation. (§ 30 Abs. 1 und Abs. 2 Nr. 1 bis 10 BSIG)

Kritische Anlagen besonders schützen

Für Betreiber kritischer Anlagen gelten zusätzliche Anforderungen. Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Für einen Infrastrukturbetreiber kann dies bedeuten, Parameter und Merkmale aus Leit-, Stellwerks- oder Fernwirkumgebungen kontinuierlich auszuwerten, soweit die betreffenden Systeme für die Funktionsfähigkeit einer kritischen Anlage maßgeblich sind, und erkannte Auffälligkeiten in definierte Bewertungs- und Incident-Response-Prozesse zu überführen. (§ 31 Abs. 1 und 2 BSIG)

Wie Angriffserkennung in der Bahn-OT aufgebaut werden kann, ohne in den Betrieb einzugreifen, beschreibt der Beitrag **„KI-gestütztes Security Monitoring“**↗.

Lieferkettenrisiken steuern

Bahnunternehmen müssen sicherheitsbezogene Risiken ihrer unmittelbaren Anbieter und Diensteanbieter berücksichtigen. Dazu zählen Hersteller von Stellwerks-, ETCS- und Fahrzeugtechnik, Instandhaltungspartner mit Fernzugriff, Telekommunikationsanbieter, Cloud- und Rechenzentrumsdienste sowie Ticketing- und Zahlungsplattformen. Neben Vertragsklauseln sind insbesondere Zugriffsregeln, Meldewege, der Umgang mit Unterauftragnehmern, Wiederanlaufverfahren und der sichere Entzug von Berechtigungen verbindlich zu regeln. (§ 30 Abs. 2 Nr. 4 und 5 BSIG)

Wie Betreiber ihre Lieferanten nach Kritikalität steuern und welche Rolle der Cyber Resilience Act dabei spielt, vertieft der Beitrag **„Cyber Resilienz in der Lieferkette“**↗.

Melde- und Krisenfähigkeit sicherstellen

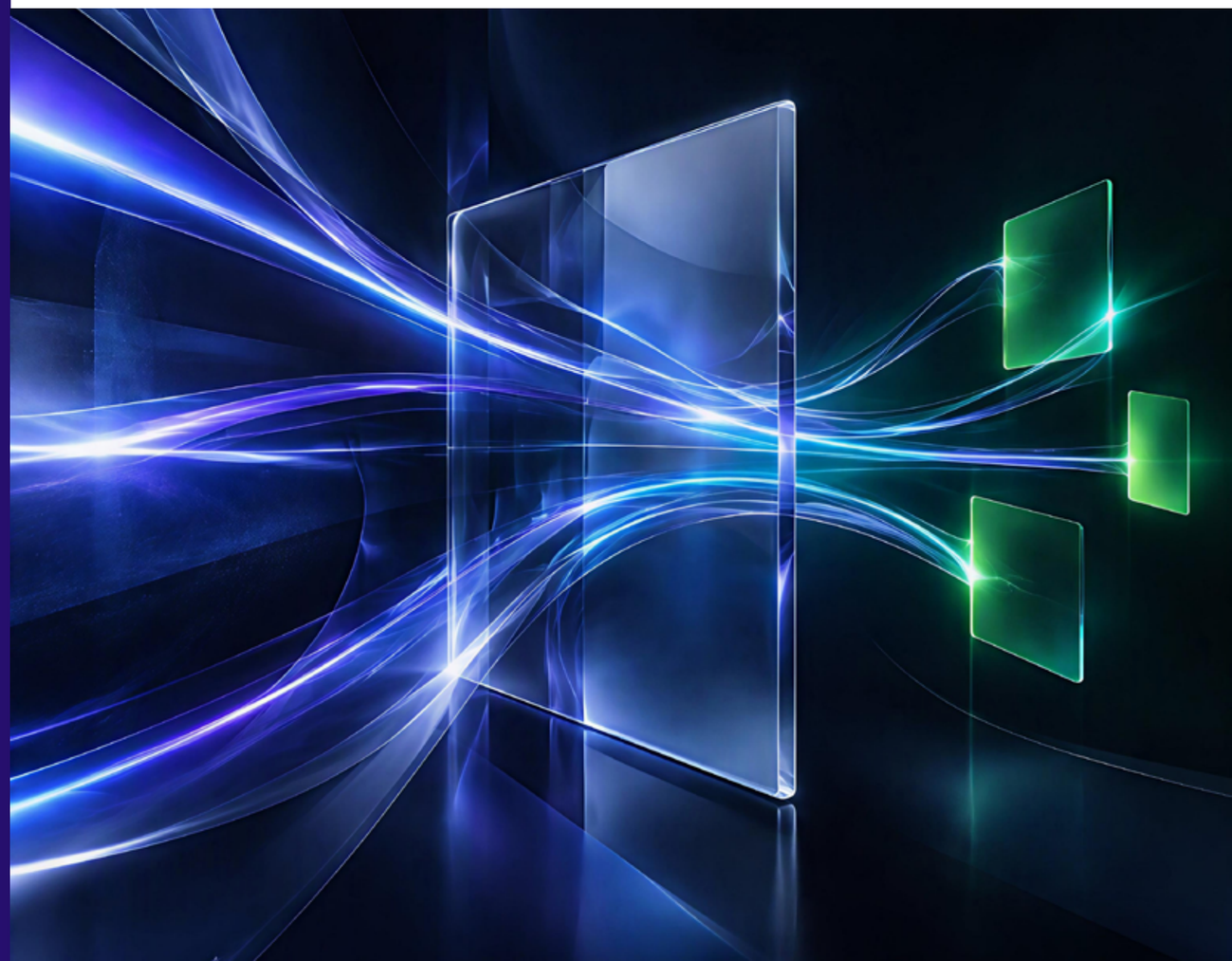
Bei erheblichen Sicherheitsvorfällen ist unverzüglich, spätestens binnen 24 Stunden, eine frühe Erstmeldung erforderlich; binnen 72 Stunden folgt die Vorfallsmeldung mit erster Bewertung. Die Abschlussmeldung ist grundsätzlich spätestens einen Monat nach der 72-Stunden-Meldung vorzulegen. Dauert der Vorfall an, tritt zunächst eine Fortschrittsmeldung an ihre Stelle. Für Vorfälle etwa in Zugdisposition oder Reisendeninformation müssen technische Analyse, betriebliche Bewertung, Recht, Kommunikation und Management deshalb bereits vor dem Ereignis in einem gemeinsamen Prozess verbunden sein. (§ 32 Abs. 1 und 2 BSIG)

Die 24-Stunden-Frist ist vor allem in der OT eine Herausforderung. Meldet das Security Monitoring eine Auffälligkeit in einem Stellwerksnetz, muss vorab geklärt sein, wer die betriebliche Auswirkung bewertet, wer über eine Isolierung entscheidet und ab wann der Betrieb auf die Rückfallebene wechselt. Diese Entscheidungskriterien sollten Security, Betrieb sowie Leit- und Sicherungstechnik gemeinsam festlegen.

Wie Krisenmanagement erfolgreich im Bahnsektor aufgebaut wird, beschreibt der Beitrag **„Krisenmanagement im Bahnsektor: Von gemeinsamen Begriffen zur Handlungsfähigkeit“**↗.

Geschäftsleitung, Nachweise und Sanktionen berücksichtigen

Die Geschäftsleitung muss Risikomanagementmaßnahmen umsetzen, überwachen und regelmäßig an Schulungen teilnehmen. Betreiber kritischer Anlagen müssen die Anforderungen nach § 30 Abs. 1 in Verbindung mit § 31 BSIG zu einem vom BSI bestimmten Zeitpunkt und danach alle drei Jahre durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachweisen. Für den ersten Nachweis, Übergangsregelungen und Ausnahmen ist die jeweilige Fallkonstellation maßgeblich. Das BSI kann Prüfungen und Abhilfemaßnahmen anordnen. Verstöße gegen zentrale Risiko-, Dokumentations- oder Meldepflichten können bei besonders wichtigen Einrichtungen mit bis zu zehn Millionen Euro und bei wichtigen Einrichtungen mit bis zu sieben Millionen Euro geahndet werden; bei mehr als 500 Millionen Euro weltweitem Gesamtumsatz gelten unter bestimmten Voraussetzungen umsatzbezogene Obergrenzen. (§ 38 Abs. 1 bis 3; § 39 Abs. 1, 3 und 4; §§ 61 und 62; § 65 Abs. 2 und Abs. 5 bis 8 BSIG)



Die Umsetzung in fünf Schritten

Ein risikoorientiertes Vorgehensmodell übersetzt regulatorische Anforderungen in ein steuerbares Transformationsprogramm für den Bahnbetrieb.

Ausgangspunkt der Umsetzung ist ein strukturiertes Vorgehen, das die regulatorischen Anforderungen mit den betrieblichen Realitäten des Bahnsektors verknüpft. Zunächst werden Betroffenheit, Scope und Verantwortlichkeiten geklärt. Anschließend wird der Ist-Zustand mit den gesetzlichen Maßnahmenbereichen abgeglichen; identifizierte Lücken werden nach Risiko, betrieblicher Wirkung und Abhängigkeiten priorisiert. Die Umsetzung erfolgt als steuerbares Programm mit klaren Ergebnissen, Ressourcen und Wirksamkeitskriterien. Aus einzelnen Pflichten wird so ein Steuerungsmodell für Cyber Resilienz und Betriebsstabilität.

1. Betroffenheit und Governance klären
Betroffene Einrichtungen, kritische Anlagen und Registrierungsanforderungen bestimmen sowie Entscheidungs-, Berichts- und Eskalationsrechte zwischen Geschäftsleitung, CISO, Betrieb, IT, OT, Einkauf, Recht und Krisenorganisation festlegen.

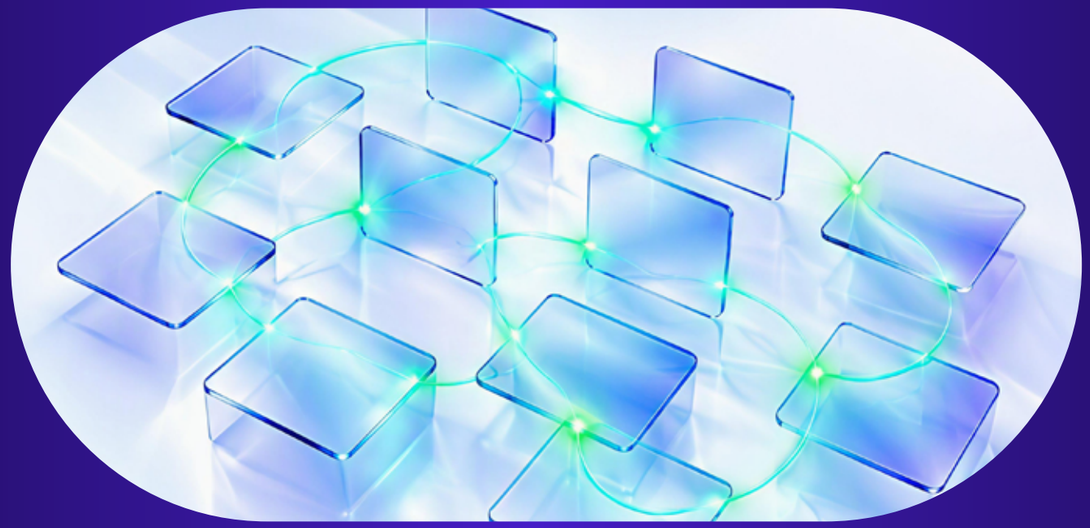
2. Kritische Bahnleistungen und Abhängigkeiten erfassen
Leistungen wie Zugdisposition, sichere Fahrwegsteuerung, Fahrzeugbereitstellung, Bahnstromversorgung und Reisendeninformation mit den zugehörigen Prozessen, IT- und OT-Systemen, Schnittstellen, Daten, Standorten, Rollen und Dienstleistern verknüpfen.

Entscheidend ist, dass die Standards aufeinander abgestimmt angewendet werden.

3. Soll-Anforderungen und Reifegrad abgleichen
Die Maßnahmenbereiche des § 30 Abs. 2 BSIG mit bestehenden ISMS-, BCM-, ITSM-, Safety-, Instandhaltungs- und Lieferantenprozessen vergleichen und Lücken nach Risiko, Auswirkungen auf Verkehrsleistung und Kapazität sowie Wiederanlaufabhängigkeiten priorisieren. **Formale Dringlichkeit allein ist dafür kein guter Maßstab.**

4. Maßnahmen als Programm steuern
Für jede Maßnahme einen verantwortlichen Owner, ein erwartetes Ergebnis, einen Termin, den Ressourcenbedarf, relevante Abhängigkeiten und ein Wirksamkeitskriterium festlegen. Ein Infrastrukturbetreiber kann beispielsweise Fernwartungszugänge absichern, Netzwerkzonen definieren und die Angriffserkennung ausbauen; ein Verkehrsunternehmen kann Wiederanlaufprioritäten für Flottenplanung, Werkstattsteuerung und Reisendeninformation festlegen.

5. Wirksamkeit testen und kontinuierlich verbessern
Wiederherstellungstests, Krisen- und Lieferantenübungen sowie kombinierte IT/OT-Szenarien durchführen. Ein geeignetes Szenario ist der gleichzeitige Ausfall von Zugdisposition und Reisendeninformation. Dabei wird geprüft, ob Ersatzverfahren greifen, priorisierte Verkehre gesteuert, Reisende konsistent informiert und die NIS2-Meldeprozesse fristgerecht ausgelöst werden. Erkenntnisse fließen systematisch in Risiken, Maßnahmen und Notfallverfahren zurück. (§ 30 Abs. 2 Nr. 3 und 6 BSIG)



Bewährte Normen schaffen ein gemeinsames Umsetzungsgerüst

Etablierte Normen helfen, die gesetzlichen Ziele in Management, IT, OT, Engineering und Safety umzusetzen.

Die gesetzlichen Anforderungen legen fest, welche Sicherheitsziele Bahnunternehmen erreichen müssen, enthalten jedoch nicht für jede technische und organisatorische Fragestellung ein vollständiges Umsetzungsmodell. Normen helfen, die Pflichten in bestehende Governance-, Engineering-, Safety- und Betriebsprozesse zu übersetzen. Entscheidend ist, dass die Standards aufeinander abgestimmt angewendet werden. Folgende Normen können für die Umsetzung relevant sein:

ISO/IEC 27001:2022

Die Norm bildet den übergreifenden Rahmen für Governance, Risikomanagement, Verantwortlichkeiten und die kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems. Für Bahnunternehmen kann sie kritische Leistungen wie Zugdisposition, Stellwerksbetrieb, Fahrzeugbereitstellung und Reisendeninformation in einem gemeinsamen Risikomodell zusammenführen.

ISO 22301:2019

Der Standard strukturiert das Business Continuity Management. Er unterstützt bei der Festlegung von Mindestbetriebszuständen, Wiederanlaufprioritäten und Ersatzverfahren. Fällt beispielsweise die zentrale Umlaufplanung aus, sollten priorisierte Verkehre, manuelle Verfahren sowie die Abstimmung zwischen Betrieb, Leitstelle und Reisendeninformation vorab festgelegt und erprobt sein. Ergänzend beschreibt der BSI-Standard 200-4 den Aufbau eines Business-Continuity-Management-Systems praxisnah und kompatibel zu ISO 22301.

IEC 62443

Die Normenreihe adressiert industrielle Automatisierungs- und Steuerungssysteme über ihren gesamten Lebenszyklus. Risikobasierte Ansätze, Defence-in-Depth sowie Zonen und Kommunikationsverbindungen sind insbesondere für Stellwerke, Fernwirktechnik sowie Fahrzeug- und Werkstattsysteme relevant. Bei älteren Systemen können Segmentierung, restriktive Übergänge, kontrollierte Fernwartung und zusätzliche Angriffserkennung fehlende Sicherheitsfunktionen kompensieren.

DIN CLC/TS 50701 (VDE V 0115-701):2024-07

Die deutsche Fassung der CLC/TS 50701:2023 überträgt Grundsätze der IEC-62443-Reihe in den Bahnkontext und verbindet Cybersecurity mit dem RAMS-Lebenszyklus nach EN 50126-1. Sie unterstützt Bahnbetreiber, Integratoren und Zulieferer bei Systemdefinition, Risikobeurteilung, Sicherheitsanforderungen und Nachweisführung sowie bei der Einbindung von Security in Entwicklung, Betrieb, Instandhaltung und Außerbetriebnahme.

Normenreihe EN 50126

Die Normenreihe bildet die Brücke zu etablierten RAMS- und Safety-Prozessen. Maßgeblich sind insbesondere DIN EN 50126-1:2025-09 zum generischen RAMS-Prozess sowie DIN EN 50126-2 in Verbindung mit der Änderung DIN EN 50126-2/A1:2025-07 zur systembezogenen Sicherheitsmethodik. Cybersecurity-Anforderungen können dadurch in bestehende Systemdefinitionen, Risikoanalysen, Abnahmen und Änderungsprozesse integriert werden, statt eine separate Security-Prozesswelt aufzubauen.

Die genannten Normen begründen nicht automatisch eine gesetzliche Erfüllungsvermutung. Sie bieten jedoch ein bewährtes Vorgehen, um gesetzliche Pflichten in vorhandene Management- und Lebenszyklusprozesse zu überführen. Auswahl und Anwendungstiefe müssen zum Geschäftsmodell, Systembestand, Risikoprofil und Reifegrad des jeweiligen Bahnunternehmens passen.



NIS2 als Hebel für einen resilienten Bahnbetrieb

Wer NIS2 konsequent an kritischen Bahnleistungen ausrichtet, stärkt mit der Compliance zugleich die Betriebsstabilität.

Strategisch bedeutsam wird NIS2 dort, wo Unternehmen ein leistungsorientiertes Steuerungsmodell aufbauen. Es bewertet Cyberrisiken anhand ihrer Auswirkungen auf Verkehrs- und Infrastrukturleistungen und priorisiert Sicherheitsmaßnahmen nach ihrem Beitrag zur Betriebsstabilität.

Dafür müssen die betrieblichen Abhängigkeiten bekannt sein. Welche Komponenten für den Bahnbetrieb tatsächlich kritisch sind, lässt sich nur bereichsübergreifend beurteilen. Infrastrukturbetreiber können Investitionen dadurch gezielter auf Leitstellen, Stellwerke oder Fernwirktechnik ausrichten, Verkehrsunternehmen auf Flottenmanagement, Werkstattsteuerung oder Reisendeninformation.

Zugleich verbindet NIS2 Steuerungsdisziplinen, die in vielen Organisationen noch getrennt betrachtet werden: Informationssicherheitsmanagement, Business Continuity Management, Incident Response, Krisenmanagement, Safety und Lieferantensteuerung. Gemeinsame Risikoszenarien und Schutzziele schaffen klarere Verantwortlichkeiten, konsistentere Entscheidungswege und eine bessere Abstimmung zwischen Geschäftsleitung, CISO, Betrieb, IT und OT.

Ob dieses Steuerungsmodell funktioniert, zeigt sich in der Praxis. Übungen, Wiederherstellungstests und Management Reviews machen sichtbar, ob kritische Leistungen auch unter Störbedingungen kontrolliert fortgeführt oder wiederhergestellt werden können. Das in Schritt 5 beschriebene Ausfallszenario eignet sich dafür als Einstieg.

Wenn ein Bahnunternehmen die NIS2-Bestimmungen umsetzt, erfüllt es seine gesetzlichen Pflichten und erhöht gleichzeitig seine operative Resilienz.

IT/OT-Konvergenz im Bahnsektor: Die Sicherheit entscheidet sich an den Übergängen

Bahnunternehmen digitalisieren Fahrzeuge, Leit- und Sicherungstechnik, Energieversorgung und Instandhaltung, und mit jedem Projekt kommen Verbindungen zwischen OT und Unternehmens-IT hinzu. Ulrich Zackor, Head of OT-Security bei DB InfraGO, nennt IT/OT-Konvergenz im anschließenden Interview ein „Buzzword aus der Beratung". Der Beitrag zeigt: Beide Welten verschmelzen nicht, entscheidend sind die Übergänge zwischen ihnen und die Frage, wie Bahnunternehmen sie so aufbauen, dass die Vernetzung beherrschbar bleibt.

*Autor: **Bernhard Barth**, Associate Partner, Wavestone*

KEY TAKEAWAYS

- **IT/OT-Konvergenz braucht kontrollierte Übergänge:** Jede Verbindung zwischen OT und Unternehmens-IT wird nach Zweck, Kritikalität und Verantwortung gestaltet.
- **Zonen und Conduits strukturieren die Kommunikation:** Steuerung, Wartung und Telemetrie laufen über getrennte Wege mit jeweils passenden Zugriffs- und Schutzmechanismen.
- **Jede Schnittstelle braucht einen verantworteten Lebenszyklus:** Anforderungen an Updates, Support und Protokollierung müssen bereits bei Beschaffung und Engineering berücksichtigt werden. Auch der spätere Rückbau ist von Anfang an vorzusehen.
- **Gemeinsame Entscheidungen:** Über IT/OT-Übergänge entscheiden Betrieb, Engineering, Safety und Cybersecurity gemeinsam und mit klar verteilten Zuständigkeiten.
- **Die OT muss auch bei Ausfall der Unternehmens-IT betriebsfähig bleiben:** Abhängigkeiten von zentralen Identitäts- und Plattformdiensten müssen begrenzt und regelmäßig getestet werden.

Konvergenz beginnt an der Systemgrenze

IT/OT-Konvergenz bezeichnet keine einheitliche Zielarchitektur, sondern die bewusste Gestaltung von Übergängen zwischen unterschiedlichen technischen und betrieblichen Logiken.

Im Bahnsektor wachsen Systeme mit sehr unterschiedlichen Anforderungen zusammen: digitale Stellwerke, European Train Control System (ETCS), Leittechnik der Bahnstromversorgung, Fahrzeug-Ferndiagnose, Instandhaltungsplattformen und cloudbasierte Analysedienste. Leit- und Sicherungstechnik ist auf Safety, Verfügbarkeit und Nachweisbarkeit ausgelegt und wird über Jahrzehnte betrieben. Unternehmens-IT und Datenplattformen ändern sich dagegen in Monatszyklen.

Der Begriff Konvergenz darf deshalb nicht als Auflösung aller Grenzen verstanden werden. Die zentrale Frage der Architektur ist, was an einer Systemgrenze passiert: Welche Daten oder Funktionen werden zu welchem Zweck übertragen und kann die Verbindung im Ereignisfall ohne betriebliche Folgen getrennt werden? Eine gute Architektur macht diese Übergänge transparent. Auch wenn eine gemeinsame Verbindung technisch bequemer wäre, bleiben Steuerung, Überwachung, Analyse und Administration getrennt.

Damit verschiebt sich die Leitfrage. Der digitale Reifegrad wird nicht durch die Zahl der angebundenen Systeme bestimmt. Maßgeblich ist vielmehr die Beherrschbarkeit ihrer Beziehungen. Konvergenz wird somit zur Gestaltungsaufgabe für das gesamte soziotechnische System aus Technik, Prozessen, Verantwortlichkeiten und Lieferketten.



Eine Zielarchitektur braucht kontrollierte Übergänge

Zonen, Conduits und getrennte Regeln für Steuerung, Wartung und Telemetrie bilden das Gerüst.

Historisch gewachsene Bahnlandschaften enthalten proprietäre Protokolle, herstellerspezifische Komponenten und Anlagen, die für lokale Nutzung entwickelt wurden. Werden solche Systeme nachträglich an zentrale Dienste angebunden, entstehen häufig Verbindungen, deren betriebliche Wirkung und Sicherheitsrisiken nur unvollständig beschrieben sind. Eine bloße Netztrennung reicht ebenso wenig wie eine pauschale Öffnung für neue Datenbedarfe.

IEC 62443 und die bahnspezifische CLC/TS 50701 liefern dafür das Modell. Systeme werden nach Funktion und Kritikalität in Zonen gegliedert. Kommunikation zwischen Zonen läuft ausschließlich über definierte Conduits, also Übergänge mit festgelegten Schutzanforderungen. Für jede Zone wird ein Ziel-Security-Level bestimmt. Innerhalb dieses Modells brauchen drei Verkehrsarten unterschiedliche Regeln:

- **Steuerbefehle** bleiben innerhalb der betrieblichen Zonen und werden nur aus den dafür vorgesehenen Bedienplätzen ausgelöst.
- **Wartungszugriffe** laufen über Jump Hosts und ein Privileged Access Management. Sie sind zeitlich befristet, werden anlassbezogen freigegeben und aufgezeichnet.
- **Telemetrie** aus sicherheitsrelevanten Zonen fließt über unidirektionale Gateways oder Datendioden in eine OT-DMZ und wird von dort weiterverteilt.

Jeder Übergang braucht einen fachlichen Zweck, eine technische Freigabe, eine Protokollierung und einen vorgesehenen Rückfallmodus. Das hilft auch bei der Weiterentwicklung: Sind die Schnittstellen versioniert und testbar, können sich Analyse- und Plattformdienste schneller entwickeln, ohne dass jede Änderung die OT berührt.

OT-Daten kontrolliert bereitstellen statt Direktzugriffe schaffen

Der Mehrwert der Konvergenz liegt in kontrolliert bereitgestellten Daten, die viele Anwendungen nutzen können, ohne dass jede einen eigenen Zugriff auf die Produktionsumgebung braucht.

Zustands- und Diagnosedaten aus Fahrzeugen, Stellwerken oder Energieanlagen können beispielsweise für Instandhaltung, Störungsanalysen oder die Optimierung des Betriebs genutzt werden. Statt dafür jeweils eigene Zugriffswege zu schaffen, können benötigte Informationen gebündelt über eine definierte Schnittstelle, etwa in der OT-DMZ, bereitgestellt werden.

Nutzbar sind diese Daten nur, wenn Herkunft, Bedeutung, Aktualität und Qualität nachvollziehbar sind. Ein Messwert ohne Bezug zu Asset, Messstelle, Betriebszustand und Zeitstempel lässt sich nur eingeschränkt interpretieren.

Gleichzeitig gilt das Prinzip der Datenminimierung: Es werden nur die tatsächlich benötigten Informationen bereitgestellt. Sensible Konfigurations- oder Topologiedaten verbleiben in der geschützten Umgebung, sofern sie für den jeweiligen Anwendungsfall nicht erforderlich sind. So lassen sich Daten sicher nutzen, ohne dass unnötige zusätzliche Zugriffswege geschaffen werden.

Der Lebenszyklus entscheidet über die Sicherheit

Jede neue Schnittstelle erzeugt Betriebs- und Schutzpflichten für Jahrzehnte.

Bahninfrastruktur wird über Jahrzehnte genutzt, während Betriebssysteme, Bibliotheken und Kommunikationskomponenten deutlich kürzeren Zyklen folgen. Diese Asymmetrie erzeugt technische Schulden, sobald Abhängigkeiten bei Beschaffung und Engineering nicht transparent gemacht werden. Eine kurzfristig leistungsfähige Lösung kann später schwer wartbar werden, wenn Updatefähigkeit, Ersatzteile oder Herstellerunterstützung fehlen.

Umso wichtiger ist die Beschaffung. Neben den Funktionen gehören eine Software Bill of Materials (SBOM), sichere Updatewege, Protokollierbarkeit, unterstützte Protokolle, ein Prozess für Schwachstellenmeldungen und verbindliche Supportzeiträume ins Lastenheft. Der Cyberresilience Act stärkt hier die Position der Betreiber: Ab Dezember 2027 verpflichtet er Hersteller unter anderem zu Sicherheitsupdates über einen festgelegten Supportzeitraum. Er gilt allerdings nur für neu in Verkehr gebrachte Produkte (siehe Beitrag **„Cyber Resilienz in der Lieferkette“**↗). Für Legacy-Systeme braucht es dokumentierte kompensierende Maßnahmen und einen Modernisierungspfad. Änderungen sollten in einer repräsentativen Testumgebung geprüft und gemeinsam von Safety, Betrieb und Security bewertet werden. Besonders wichtig ist die Rückbaubarkeit. Schnittstellen, Konten, Zertifikate und Datenflüsse müssen mit dem Ende eines Anwendungsfalls entfernt oder angepasst werden können.

Ein gemeinsames Betriebsmodell übersetzt zwischen IT und OT

Technische Übergänge brauchen organisatorische Gegenstücke mit klaren Entscheidungsrechten.

IT, OT, Engineering, Instandhaltung, Betrieb und Cybersecurity bewerten Änderungen aus verschiedenen Blickwinkeln. Diese Trennung ist im Bahnsektor teils gewollt, etwa durch die Unabhängigkeit der Safety-Bewertung. Wirksam wird sie mit einem gemeinsamen Verfahren, einer eindeutigen Verantwortung für Systeme und Schnittstellen und einem Mandat, Risiken über Bereichsgrenzen hinweg zu priorisieren.

Das Betriebsmodell legt fest, wer Datenflüsse und Übergänge freigibt, Änderungen bewertet, Wartungsfenster koordiniert und im Falle von Abweichungen Entscheidungen trifft. Die Prozesse für Änderungen (Change), Konfigurationen (Configuration) und Störungen (Incident) greifen auf dieselbe Abhängigkeitssicht zu, einschließlich der OT-Komponenten und ihrer Übergänge. OT-Security-Spezialisten, die sowohl den Bahnbetrieb als auch die Zulassungslogik kennen und technische Befunde in betriebliche Auswirkungen übersetzen können, machen die Auswirkungen für Entscheider verständlich.

In dieses Modell gehören auch Dienstleister und Hersteller, da Fernwartung, Softwarepflege und Störungsanalyse privilegierte Zugänge zu kritischen Umgebungen schaffen. Verträge, technische Kontrollen und operative Verfahren müssen deshalb aufeinander abgestimmt sein. **Ein formal begrenzter Zugriff ist nur dann wirksam, wenn Freigabe, Nutzung, Überwachung und Beendigung im Betrieb reibungslos funktionieren.**

Resilienz wird zur Eigenschaft der Gesamtarchitektur

Im Bahnbetrieb heißt der sichere Zustand „Halt". Resilienz verlangt, dass der Betrieb auch unterhalb der vollen Funktion weiterlaufen kann.

Leit- und Sicherungstechnik ist nach dem Failsafe-Prinzip gebaut: Im Zweifel geht ein Signal auf Halt. Das schützt Menschen, bringt aber den Zugverkehr zum Stillstand. Zwischen sicherem Abschalten und kontrolliertem Weiterbetrieb besteht damit ein Zielkonflikt, den die Architektur vorab auflösen muss. Zentrale Plattformen schaffen zudem neue gemeinsame Ausfallpunkte. Besonders kritisch sind Identitätsdienste: Hängen Anmeldungen an OT-Bedienplätzen oder Engineering-Stationen sowie Wartungszugänge am Active Directory der Unternehmens-IT, legt ein Ransomware-Angriff auf die IT auch die OT lahm.

Eine eigene Identitätsdomäne für die OT, lokale Notfallkonten und offline vorgehaltene Konfigurationen und Wiederherstellungsmedien sind deshalb Grundvoraussetzungen. Für jede kritische Betriebsleistung werden die Degradationsstufen beschrieben: Was funktioniert ohne Datenplattform, was ohne Verbindung zur Betriebszentrale, und welche Entscheidungen sind lokal möglich? Übungen prüfen diese Stufen gemeinsam mit Betriebszentrale, Instandhaltung, IT-Betrieb und OT-Verantwortlichen (siehe Beitrag ***„BCM auf die Schiene bringen"***↗).

Ein System kann eingeschränkt weiterarbeiten, Daten später synchronisieren oder in einen sicheren Betriebsmodus wechseln. Solche Zustände müssen bereits im Design vorgesehen sein. Jedes Bahnunternehmen müsste demnach nachweisen können, dass seine OT bei vollständigem Ausfall der Unternehmens-IT betriebsfähig bleibt, und dieses Szenario mindestens einmal real üben. **Ein solcher Test zeigt erfahrungsgemäß Abhängigkeiten, die in keiner Dokumentation stehen.**

Der Weg zur Konvergenz folgt dem betrieblichen Nutzen

Am Anfang steht das Inventar der Übergänge. Eine vollständige Zielarchitektur auf dem Papier ist kein guter Startpunkt.

Ein flächendeckendes Großprogramm ohne Überblick über die bestehenden Verbindungen erhöht zunächst die Komplexität. Der pragmatische Einstieg ist ein Inventar aller IT/OT-Übergänge mit Zweck, Verantwortlichem und Kritikalität, ergänzt durch passives Monitoring, das auch undokumentierte Verbindungen sichtbar macht. Auf dieser Basis werden die Übergänge priorisiert, die kritische Betriebsleistungen berühren.

Neue Anwendungsfälle sollten als Piloten unter realen Bedingungen umgesetzt werden. Eine funktionierende Datenübertragung reicht dabei als Erfolgskriterium nicht aus. Dazu gehören auch ein benannter Verantwortlicher für jeden Übergang, ein beherrschter Änderungsprozess einschließlich Zulassungsfragen und eine nachgewiesene Rückfallfähigkeit. Die Erkenntnisse sollten in verbindliche Architekturprinzipien für Neubau und Modernisierung einfließen.

Das gilt besonders für den laufenden Rollout digitaler Stellwerke und von ETCS. Dort werden die Übergänge der nächsten Jahrzehnte festgelegt. Heute lassen sie sich noch mit vertretbarem Aufwand richtig gestalten.

OT-Security in der Bahn: „Wir brauchen weniger Know-how und mehr Do-how“

Ulrich Zackor verantwortet die OT-Security bei DB InfraGO. Im Gespräch erklärt er, warum er den Begriff IT/OT-Konvergenz für ein Schlagwort aus der Beratung hält und weshalb in der OT die Umsetzung im laufenden Betrieb mehr zählt als das nächste Konzept.



Ulrich Zackor, Head of OT-Security bei DB InfraGO

Herr Zackor, Sie verantworten die OT-Security bei DB InfraGO. Wie ist Ihre Rolle organisatorisch verankert und worauf liegt Ihr Fokus?
Unsere OT-Security ist bewusst im operativen Bereich verortet, also im COO-Ressort – und nicht im klassischen CISO-Bereich. Der Grund ist einfach: Wir sind kein reiner Governance- oder Stabsbereich, sondern der „Transmissionsriemen“ ins operative Geschäft. Wir müssen Sicherheit dort umsetzen, wo die Systeme tatsächlich laufen – entlang der gesamten Infrastruktur und Wertschöpfungskette.
Das bedeutet auch, dass wir interdisziplinär arbeiten müssen. Erfolgreiche OT-Security braucht gleichzeitig Eisenbahninfrastruktur-Erfahrung, IT-Know-how und Security-Kompetenz. Das kann keine Einzelperson leisten – dafür braucht es gut verzahnte Teams.

IT/OT-Konvergenz gilt als zentraler Trend. Teilen Sie diese Einschätzung?
Ehrlich gesagt: nur sehr eingeschränkt. Der Begriff „IT/OT-Konvergenz“ ist aus meiner Sicht oft eher ein Buzzword aus der Beratung. Natürlich nutzen wir zunehmend IT in der OT, aber das bedeutet nicht, dass beide Welten konvergieren.
Die Unterschiede sind fundamental. OT-Systeme sind häufig safety-kritisch, sie haben extrem lange Lebenszyklen und die Priorität liegt auf Verfügbarkeit und nicht auf Vertraulichkeit. Diese beiden Welten lassen sich nicht einfach zusammenführen. Deshalb haben wir uns auch organisatorisch bewusst nicht konvergent aufgestellt



– gleichwohl stehen wir mit den Kollegen aus dem CIO- und CISO-Bereich in engem Austausch, um Wissen und Erfahrungen zu transferieren.

Trotzdem profitieren Sie von der IT-Welt, oder nicht?
Doch, absolut. Aber selektiv. Wir übernehmen beispielsweise ITIL-Strukturen und bewährte Prinzipien wie Identity and Access Management oder Zero Trust.
Was nicht funktioniert, ist ein einfaches Übertragen von Techniken oder Geschwindigkeiten. In der IT kann ich zentral patchen und skalieren. In der OT bedeutet ein Patch unter Umständen einen Vor-Ort-Einsatz an der Anlage, Abstimmung mit Zulassungsbehörden und mögliche Risiken für den laufenden Betrieb. Das ist eine völlig andere Realität.

Was macht OT-Security im Bahnkontext so besonders herausfordernd?
Hier kommt vieles zusammen. Wir sind eine Flächenorganisation – unser „Werksgelände“ ist quasi ganz Deutschland. Wir betreiben teilweise jahrzehntealte Technik, viele Anlagen sind individuell gebaut. Gleichzeitig bewegen wir uns in einem hochregulierten Umfeld, in dem Änderungen direkte Auswirkungen auf Zulassungen haben können.
Hinzu kommt der kontinuierliche Betrieb: Die Bahn läuft rund um die Uhr, es gibt kaum Stillstand für längere Wartungs- oder Instandhaltungsfenster, von unserem neuen Generalsanierungskonzept einmal abgesehen. Ein gutes Beispiel ist das Patchmanagement. **Während man in der IT über Stunden oder Tage spricht, reden wir in der OT eher über Monate – oder im Extremfall Jahre, wenn man notwendige Zulassungen berücksichtigt.**

Wie gehen Sie mit Bedrohungen um – insbesondere vor dem Hintergrund geopolitischer Spannungen?
Die Bedrohungslage ist dauerhaft hoch – und sie ist real. Für uns war WannaCry 2017 ein Weckruf, Log4j 2021 eine erneute Bestätigung, und die Welt im Jahr 2026 ist noch herausfordernder geworden. Als Betreiber kritischer Infrastruktur und Anlagen stehen wir automatisch im Fokus – wirtschaftlich, gesellschaftlich und geopolitisch. Die Bahn ist Rückgrat der Mobilität, essenziell für die Wirtschaft und zunehmend relevant für verteidigungspolitische Logistik in Deutschland wie in Europa. Das macht uns zu einem attraktiven Ziel. Angriffe finden täglich statt – und die erfolgreiche Verteidigung auch.

Was bedeutet das für Ihre Sicherheitsstrategie?
Zum einen setzen wir auf Professionalität und Routine. Wir sind seit vielen Jahren KRITIS-Betreiber und verfügen über etablierte Prozesse, regelmäßige Audits, feste Meldewege und eingespielte Krisen- und Notfallteams.
Zum anderen spielt Resilienz eine zentrale Rolle. Sicherheit denken wir nicht nur im Cyberraum, sondern auch physisch. Es geht um den Schutz der Infrastruktur als Ganzes, um Segmentierung, mehrschichtige Verteidigungsansätze und organisatorische Resilienz.

Wie organisieren Sie die Zusammenarbeit im Ernstfall?
Bei sicherheitsrelevanten Vorfällen aktivieren wir ein Security Incident Management Team. In diesem Gremium bringen wir alle relevanten Perspektiven zusammen – von der OT über die IT bis hin zur physischen Sicherheit und den operativen Einheiten, vom CTO über den CISO bis hin zum Eisenbahnbetriebsleiter.
Die Entscheidungen werden schnell und pragmatisch und mit allen relevanten Fachbereichen getroffen. Das ist entscheidend, insbesondere wenn Safety-Aspekte betroffen sind.

Wo sehen Sie die größten Erfolgsfaktoren für OT-Security?
Ein zentraler Punkt ist die Umsetzung statt reiner Konzeptarbeit. Ich sage immer: Wir brauchen weniger Know-how und mehr Do-how. Wir wissen häufig sehr genau, was zu tun wäre. Die Herausforderung ist, es unter realen Bedingungen umzusetzen – im laufenden Betrieb, mit bestehenden Systemen und unter regulatorischen Rahmenbedingungen. Hierbei hilft das richtige „Macher-Mindset“ in Kombination mit einem kühlen Kopf für reflektierte und zügige Entscheidungen.
Ein weiterer Erfolgsfaktor ist Awareness. Viele Probleme sind erstaunlich banal, etwa nicht geänderte Default-Passwörter. Der Mensch bleibt dabei gleichzeitig sowohl größter Risikofaktor als auch wichtigster Lösungshebel.
Hinzu kommt die Bedeutung von Projektmanagement. Gute Projektmanager sind oft der Unterschied zwischen Erfolg und Misserfolg. Sie entscheiden darüber, ob Maßnahmen wirksam umgesetzt werden oder ob technische Schulden entstehen.
Und schließlich spielt Pragmatismus eine große Rolle. Eine 80-prozentige Lösung, die tatsächlich durchgängig Ende-zu-Ende umgesetzt ist, ist deutlich wertvoller als eine theoretisch perfekte Lösung, die nie realisiert wird.

Welche Empfehlungen geben Sie anderen Infrastrukturbetreibern?
Ganz klar: umsetzen und üben statt nur planen. **Papier schützt keine Infrastruktur.** Gleichzeitig müssen realistische Erwartungen entwickelt werden. Die Bedrohung ist nicht hypothetisch, sondern konkret. Die entscheidende Frage ist nicht, ob etwas passiert, sondern wann. Das erfahren wir täglich aus den Medien.
Darüber hinaus ist der Austausch zwischen Organisationen entscheidend. Länder wie Finnland zeigen, wie wichtig Vernetzung zwischen Zivilgesellschaft, Wirtschaft und staatlichen Institutionen, gemeinsames Üben und offener Austausch sind, um Resilienz wirklich zu stärken.

Abschließende Frage: Was treibt Sie persönlich in diesem Feld an?
Die Herausforderung selbst. OT-Security ist in der heutigen Welt mit all ihren Herausforderungen eines der spannendsten Themen überhaupt, weil Technik, Betrieb und Sicherheit so eng zusammenkommen.
Am Ende geht es um etwas sehr Konkretes: die Verfügbarkeit und Stabilität kritischer Infrastruktur und damit um das Funktionieren unserer Gesellschaft. Sinnstiftende Arbeit erleben wir bei der DB InfraGO und insbesondere im OT-Security-Bereich tagtäglich, was unglaublich motivierend ist – noch dazu in Teams mit enorm hoher Identifikation mit ihrer Arbeit und dem Beitrag für sichere Mobilität im Herzen Europas.

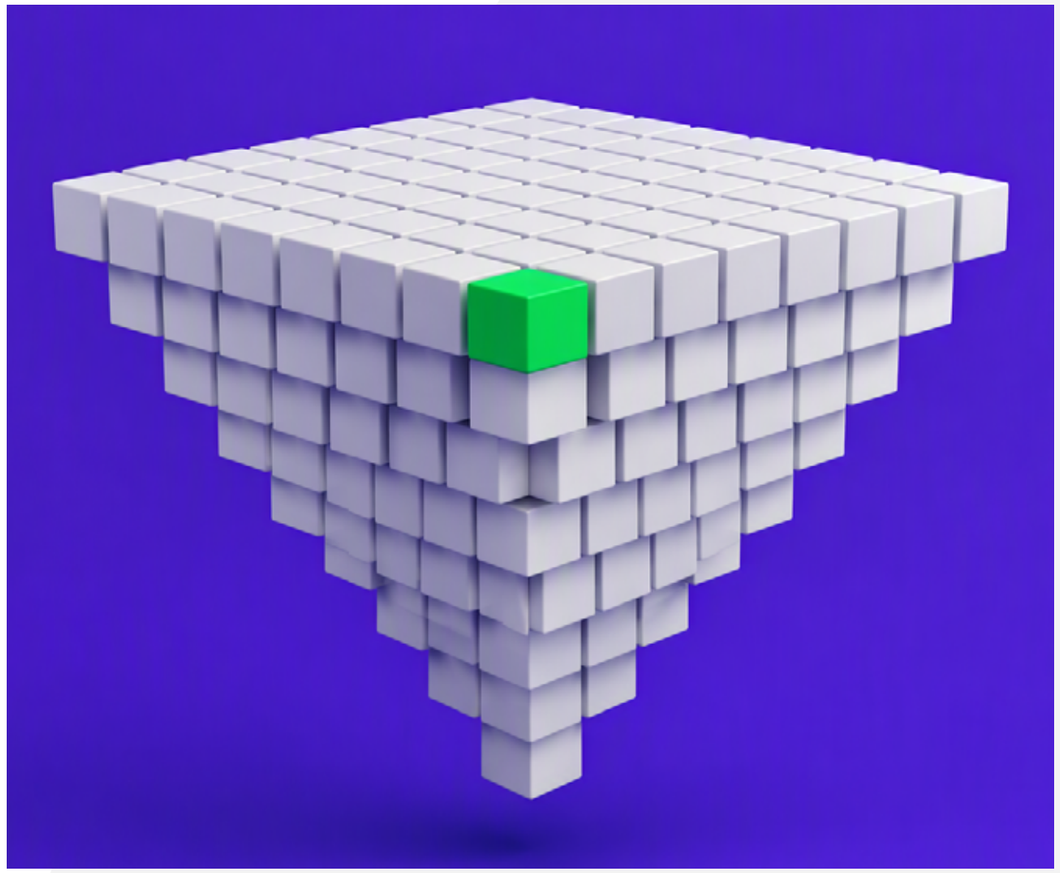
Am Ende geht es nicht um perfekte Konzepte, sondern darum, dass die Systeme 24/7 laufen. Und dass sie es auch im Ernstfall tun.

Ulrich Zackor, Head of OT-Security bei DB InfraGO

Assetmanagement im Bahnsektor: Die Grundlage jeder Sicherheitsentscheidung

Bahnunternehmen vernetzen langlebige Betriebsanlagen zunehmend mit IT- und OT-Systemen. Damit wächst die Zahl der Komponenten, die sie kennen müssen, um den Betrieb zu schützen und Störungen schnell zu beheben. Der Beitrag beschreibt, welche Assetdaten dafür nötig sind und wie sie aktuell bleiben.

Grundlage ist ein Gespräch mit einem OT-Security-Experten aus der Fertigungsindustrie.
Autor: **Markus Wendl**, *Manager, Wavestone*



KEY TAKEAWAYS

- **Ohne Inventar keine Steuerung:** Segmentierung, Angriffserkennung, Entstörung und Wiederanlauf setzen voraus, dass ein Bahnunternehmen seine Assets und deren Abhängigkeiten kennt.
- **Auch zeitweise verbundene Assets zählen:** Diagnosegeräte von Dienstleistern, Wechseldatenträger und Fahrzeuge, die nur im Depot erreichbar sind, können Teil eines Angriffswegs werden. Ein Inventar, das nur dauerhaft vernetzte Geräte erfasst, greift zu kurz.
- **Passiv erfassen, gezielt prüfen:** In der Bahn-OT kann aktives Scanning ältere Steuerungen stören. Die Ersterfassung beginnt deshalb passiv. Aktive Abfragen folgen nur abgestimmt und in Wartungsfenstern.
- **Schlankes Datenmodell:** Wenige Pflichtfelder, die zuverlässig gepflegt werden, sind wertvoller als ein vollständiges Modell, das niemand aktuell hält. Gepflegt wird am besten dort, wo ohnehin gearbeitet wird, etwa beim Instandhaltungsauftrag.
- **Die Organisation ist die größere Hürde:** Die Technik zur Erfassung ist verfügbar. Schwieriger ist es, die Verantwortung für Assetdaten über Beschaffung, Betrieb, Instandhaltung und Security hinweg festzulegen, besonders bei Fahrzeugen und Infrastrukturelementen wie Weichen oder Signalen mit mehreren Verantwortlichen.

Steuerungsfähigkeit beginnt mit der Kenntnis der eigenen Assets

Ohne ein sauber gepflegtes Assetmanagement fehlt Bahnunternehmen die Grundlage, kritische Leistungen sicher zu steuern und Störungen gezielt zu beheben.

Bahnunternehmen operieren in hochkomplexen, historisch gewachsenen IT- und OT-Landschaften. Fahrzeuge, Stellwerke, Leit- und Sicherungstechnik, Kommunikationsnetze und unterstützende IT greifen ineinander. Eine Störung wird deshalb häufig zuerst als betriebliche Einschränkung oder Monitoring-Alarm sichtbar. Ob die Ursache in einer Anwendung, einer Netzwerkkomponente, einer Firmware oder einem physischen Gerät liegt, bleibt ohne konsistente Assetdaten zunächst offen.

Assetmanagement stellt die Verbindung vom Geschäftsprozess über Systeme und Anwendungen bis zur einzelnen Komponente her. Mit dieser Verbindung lässt sich beantworten, welche betriebliche Leistung von einem Asset abhängt, welche Folgen sein Ausfall hat und wo Schutz- oder Wiederherstellungsmaßnahmen ansetzen müssen. **Der Maßstab ist deshalb, ob das Unternehmen seine kritischen Leistungen auf Basis dieser Daten steuern kann.** Die reine Zahl der gepflegten Datensätze sagt darüber wenig aus.

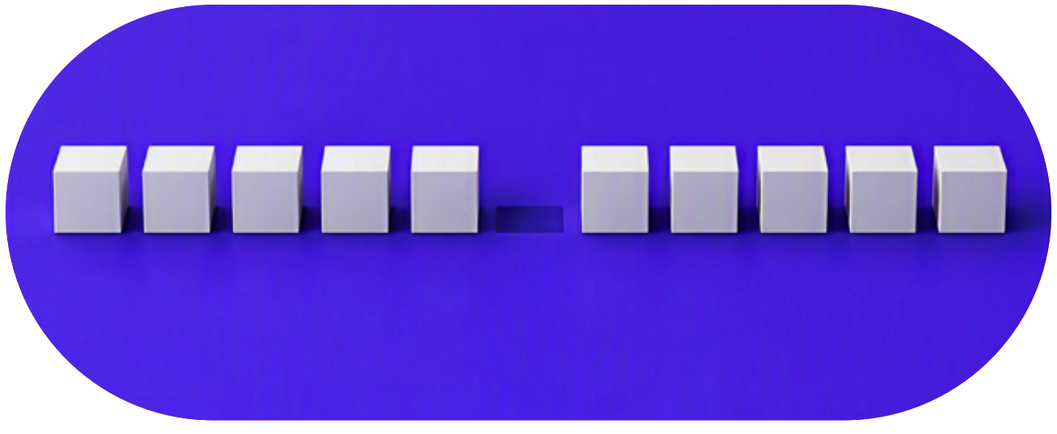
Transparenz muss vernetzte und auch verborgene Assets erfassen

Die größten Lücken liegen bei Komponenten, die nur zeitweise verbunden sind, sowie bei fehlenden Beziehungen zwischen Assets.

Historisch gewachsene OT-Landschaften enthalten blinde Flecken: proprietäre Altsysteme, isolierte Anlagen, drahtlos angebundene Komponenten oder Geräte, die nur zeitweise verbunden werden. Auch ein nicht dauerhaft vernetztes Asset kann Teil eines Angriffswegs werden. Im Bahnbetrieb betrifft das vor allem den Alltag von Instandhaltung und technischer Planung: Wartungs- und Diagnosegeräte von Dienstleistern, die nacheinander an verschiedene Anlagen angeschlossen werden, Wechseldatenträger für Software und Konfigurationen sowie Fahrzeuge, deren Steuergeräte nur im Depot oder über Funk erreichbar sind. Eine Definition, die nur Assets mit Netzwerkstecker erfasst, greift deshalb zu kurz.

Zugleich erhöht IT/OT-Konvergenz den Transparenzbedarf. Der Experte beschreibt den Ausgangspunkt klar:*„Durch die Konvergenz entstehen zusätzliche Datenflüsse und damit neue Anforderungen an Transparenz, Governance und Asset-Management-Prozesse.“* Die Grundfrage ist in Fertigung und Bahn dieselbe, und auch die Strukturen ähneln sich: Ein hochautomatisiertes Werk ist gewissermaßen Bahninfrastruktur im Kleinen. Die Unterschiede liegen vor allem in den Rahmenbedingungen. Bahnanlagen haben Übergänge zu Netzen anderer Betreiber, unterliegen Zulassungspflichten und haben Lebenszyklen von mehreren Jahrzehnten.

Transparenz umfasst deshalb Hardware, Software, Firmware und Konfigurationen sowie die Beziehungen zwischen Assets. Eine Software Bill of Materials (SBOM) und eine Hardware Bill of Materials (HBOM) erweitern diese Sicht bis auf einzelne Softwarebibliotheken und Bauteile. So lässt sich bei einer neu veröffentlichten Schwachstelle schnell feststellen, welche Anlagen betroffen sind.

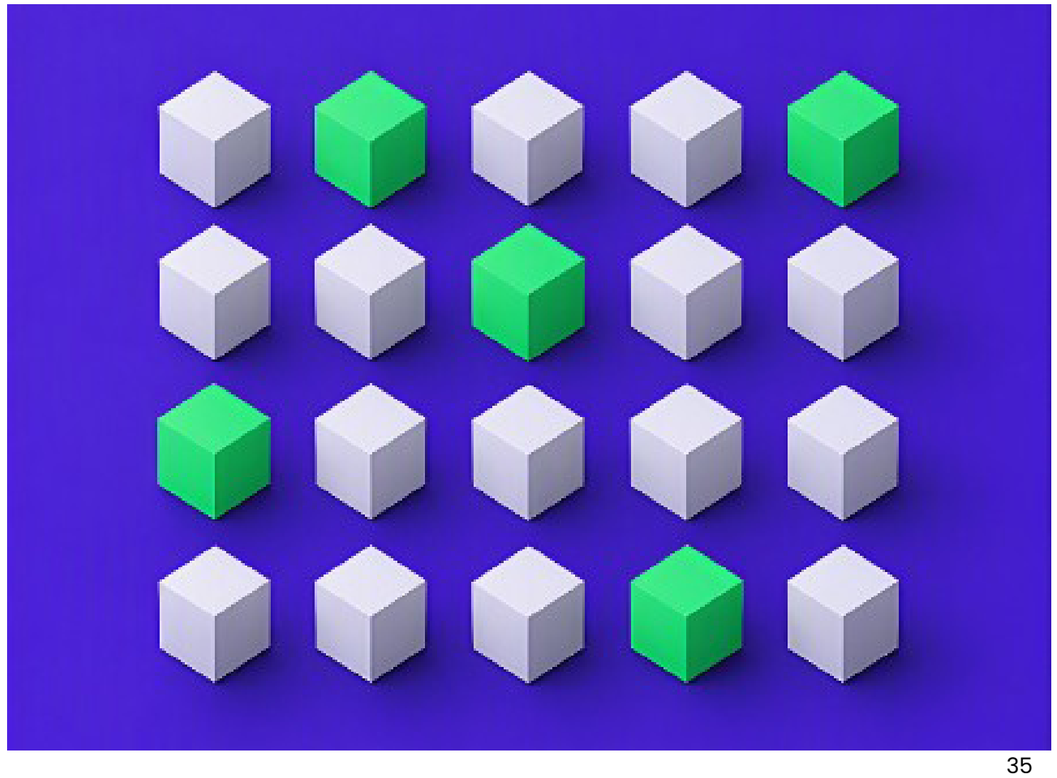


Ein schlankes Datenmodell trägt über den gesamten Lebenszyklus

Wenige Pflichtfelder, die zuverlässig gepflegt werden, sind mehr wert als ein vollständiges Modell, das niemand aktuell hält.

Die Erfassung sollte bereits beginnen, bevor ein Asset beschafft oder installiert wird. Hersteller, Modell, vorgesehener Einsatz, Firmware, Schutzbedarf und erreichbares Security Level lassen sich schon in der Planung prüfen. So werden ungeeignete oder absehbar abgekündigte Komponenten früh erkannt. Im Betrieb kommen Status, Standort, Verantwortung für Betrieb und Instandhaltung, Konfiguration und Kommunikationsbeziehungen hinzu. Lagerung, Reparatur, Austausch und Rückbau müssen ebenso nachvollziehbar bleiben wie die Historie früherer Zuordnungen.

Gute Datenqualität beginnt mit einem bewusst begrenzten Pflichtdatenmodell. Mindestens erforderlich sind eine eindeutige Identität, der genaue Standort, die verantwortliche Stelle, der Lifecycle-Status und die technischen Merkmale je Assetklasse. Der Experte fasst den langfristigen Nutzen zusammen: *„Langfristig ermöglicht eine standardisierte Datenbasis eine deutlich effizientere Verwaltung des gesamten OT-Lebenszyklus.“* Vollständigkeit bedeutet dabei nicht, jedes denkbare Feld zu füllen. Ein Asset-Tool ist weder eine Ablage für beliebige Dokumente noch ein Speicher für Zugangsdaten. Erfasst wird, was für Steuerung, Schutz, Betrieb und Nachweise tatsächlich benötigt wird.

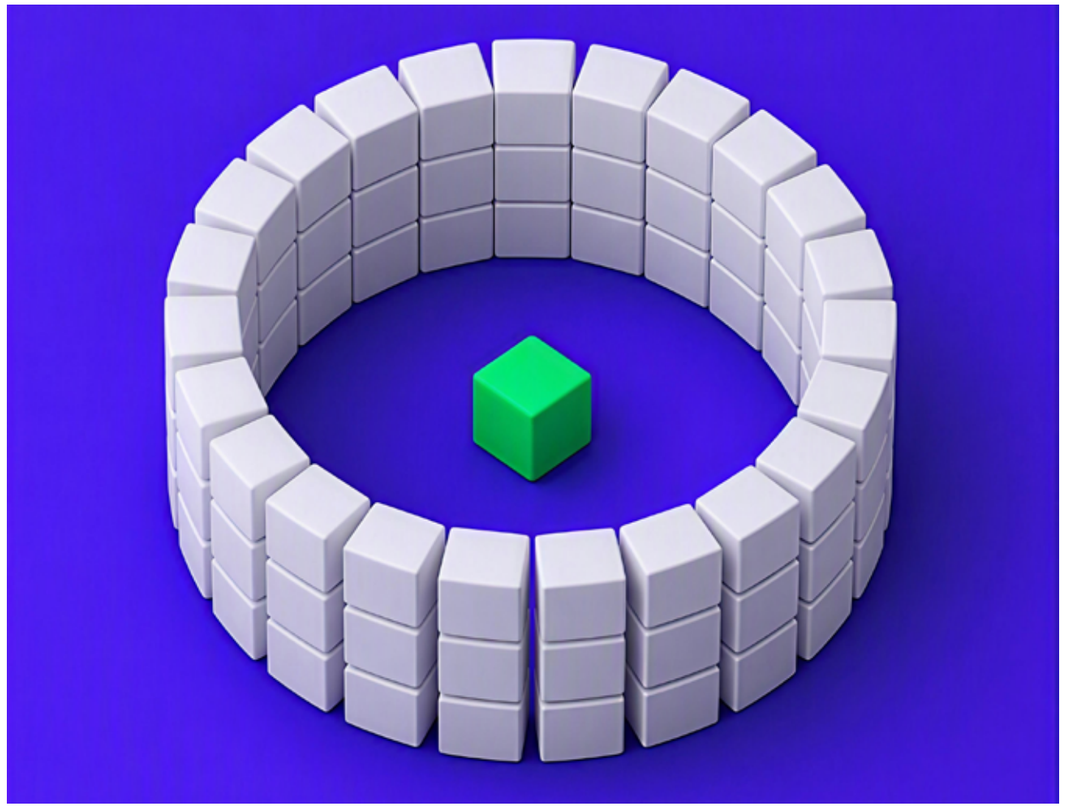


Dieselben Daten tragen Schutz und Entstörung

Assetdaten werden in der Prävention ebenso gebraucht wie im Störungsfall.

Cybersecurity braucht bekannte Assets, um Schutzbedarf und Schwachstellen zu bewerten. Segmentierung nach IEC 62443 und der bahnspezifischen CLC/TS 50701 setzt voraus, dass Zonen, Kommunikationsbeziehungen und das erforderliche Schutzniveau bekannt sind. Das Monitoring braucht den technischen und betrieblichen Kontext eines Assets, damit Schwellwerte sinnvoll gesetzt und Alarme priorisiert werden. Fehlen Kritikalität und Abhängigkeiten, erzeugt es Fehlalarme in großer Zahl, und die Analysten verlieren den Überblick.

Im Störungsfall brauchen die Einsatzkräfte dieselben Daten. Sie müssen schnell erkennen, welches Gerät betroffen ist, wo es steht, welche Komponenten verbunden sind und wer Betrieb oder Instandhaltung verantwortet. In heterogenen Bahnlandschaften verkürzt eine standardisierte oder zumindest geclusterte Dokumentation die Entstörungszeit deutlich. Für das Notfall- und Krisenmanagement zeigen die Assetdaten zudem, welche Leistungen beim Wiederanlauf Vorrang haben. Assetmanagement verbindet damit Prävention, Response und Recovery in einer konsistenten Informationsbasis.



Governance und Akzeptanz entscheiden über die Datenqualität

Ein Tool allein hält kein Inventar aktuell. Dafür braucht es verbindliche Regeln und einen erkennbaren Nutzen für die Menschen, die pflegen.

Organisatorisch braucht es ein unternehmensweites Datenmodell, eine klare Pflegeverantwortung und festgelegte Übergaben zwischen Beschaffung, Engineering, Betrieb, Instandhaltung und Cybersecurity. Technisch dient das Assetmanagement als führende Quelle. Discovery-Werkzeuge, Verzeichnisdienste, Schwachstellenmanagement, Monitoring und Incident Management liefern Daten zu oder nutzen sie über standardisierte Schnittstellen. Unser Gesprächspartner betont die Bedeutung herstellerübergreifender Standards: *„Standardisierte Schnittstellen und offene Architekturen erhöhen den Wettbewerb, schaffen mehr Flexibilität und senken langfristig die Kosten für Betrieb und Modernisierung der Produktionsanlagen.“* Für den Bahnsektor gilt das umso mehr: Bei Lebenszyklen von mehreren Jahrzehnten wechseln Hersteller und Produktgenerationen mehrfach, während die Anlagen weiterlaufen.

Automatisierte Erkennung findet Geräte und technische Merkmale. Standort, Nutzungskontext und Verantwortung kann sie aber oft nicht zuverlässig bestimmen. Ein Beispiel: Ein passiver Sensor erkennt eine Steuerung im Netz einer Stellwerks-Außenanlage. Er erkennt nicht, an welcher Betriebsstelle sie steht, welche Weichen daran hängen und ob der Hersteller oder der Instandhaltungsbezirk sie betreut. Wird nachts bei einer Störung ein Ersatzteil mit anderem Firmware-Stand eingebaut, weiß das zunächst nur der Techniker vor Ort. Dieses Wissen muss strukturiert in das Inventar einfließen. Der Experte sieht die organisatorische Seite als größere Hürde: *„Die technischen Fragestellungen sind meist einfacher zu lösen als die organisatorischen.“* Die Erfahrung zeigt: Assetdaten werden dann gepflegt, wenn die Pflege Teil eines Arbeitsschritts ist, der ohnehin stattfindet. Wer eine Komponente tauscht, bestätigt im Instandhaltungsauftrag die neue Seriennummer und den Firmware-Stand. Wer eine Änderung freigibt, aktualisiert die Kommunikationsbeziehungen. Der Nutzen zeigt sich für die Pflegenden direkt, etwa wenn bei der nächsten Störung die Daten vor Ort verfügbar sind.

Den Bestand schrittweise erfassen

Neue Standards gelten sofort für alle Neuplanungen. Der Bestand wird nach Kritikalität schrittweise erfasst.

Ein über Jahrzehnte gewachsener Bestand lässt sich nicht in einem Big Bang bereinigen. In der Bahn-OT beginnt die Erfassung deshalb mit passiver Netzwerküberwachung: Sensoren lesen den Datenverkehr mit, ohne selbst Anfragen zu senden. Aktives Scanning kann ältere Steuerungen überlasten oder zum Absturz bringen. Es bleibt gezielten, mit dem Betrieb abgestimmten Abfragen in Wartungsfenstern vorbehalten. **Transparenz macht technische Schulden zunächst sichtbar, bevor sie beseitigt werden können.**

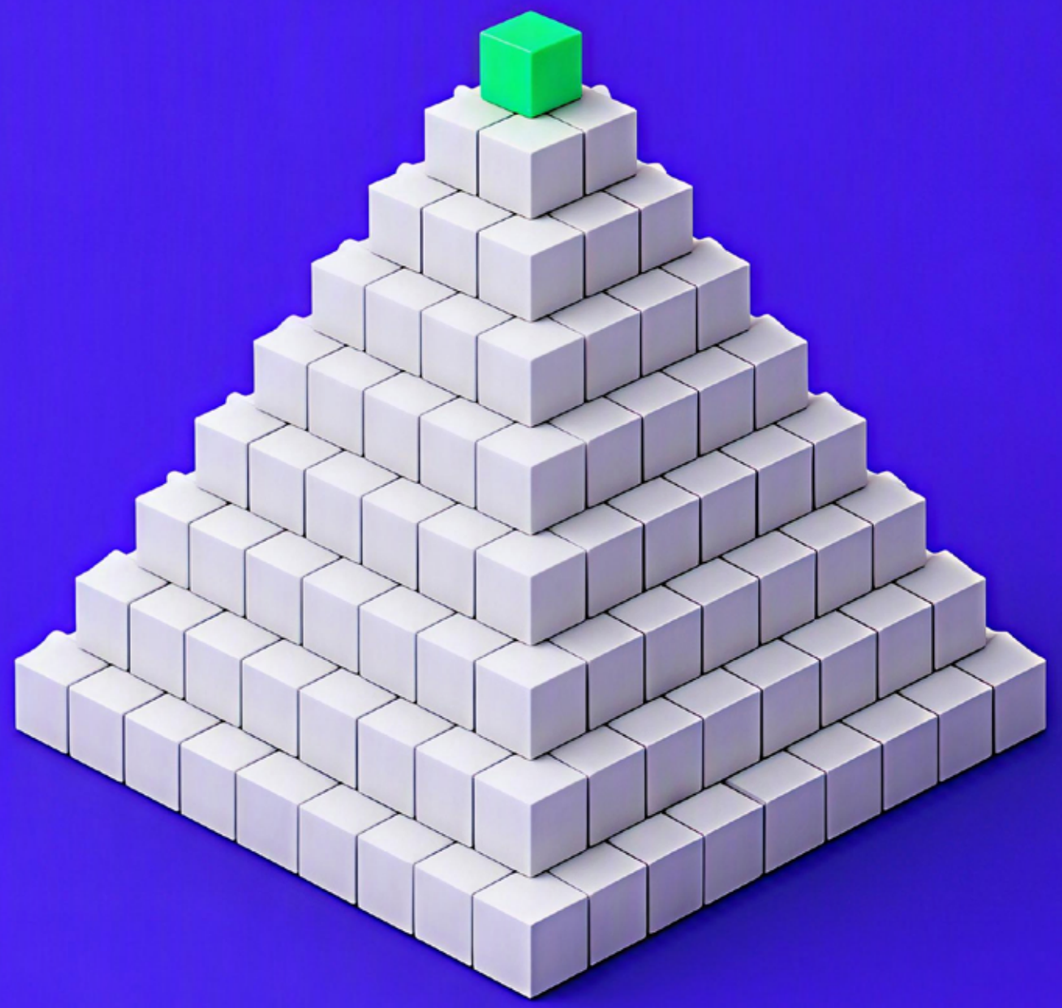
Die technische Erfassung wird durch Prüfung vor Ort und fachliche Zuordnung ergänzt. Bei Streckenaußenanlagen, die über das gesamte Netz verteilt sind, ist dieser Aufwand erheblich. Er sollte deshalb nach Kritikalität priorisiert und mit ohnehin anstehenden Instandhaltungsgängen verbunden werden.
Für Legacy-Systeme braucht es eine bewusste Entscheidung: Sie werden erfasst und über kompensierende Maßnahmen abgesichert, oder sie werden im nächsten geeigneten Erneuerungszyklus modernisiert. Adapter- und Wrapper-Konzepte können bestehende Systeme schrittweise in offenere Architekturen integrieren. Entscheidend ist, neue Standards sofort verbindlich für alle Neuplanungen zu machen und den Bestand priorisiert nach Kritikalität zu entwickeln. Der Experte empfiehlt dazu: *„Nicht zu lange planen, sondern früh pilotieren."* Eine Pilotanlage zeigt früher als alle theoretischen Zielbilder, welche Daten tatsächlich gebraucht werden und wo die Zusammenarbeit zwischen IT und OT hakt.

Gepflegte Assetdaten machen Schwachstellen und Muster sichtbar

Wer seinen Bestand kennt, kann auf neue Schwachstellen in Stunden reagieren.

Der unmittelbare Security-Nutzen eines gepflegten Inventars zeigt sich bei jeder neuen Schwachstellenmeldung. Liegen SBOM und Firmware-Stände vor, lässt sich automatisiert abgleichen, welche Anlagen betroffen sind. Ohne diese Daten beginnt jedes Mal eine manuelle Suche über Fachbereiche und Hersteller hinweg. Mit der Zeit kommen historische Daten hinzu. Werden Asset- und Störungsdaten verknüpft, lassen sich wiederkehrende Fehler bestimmten Komponenten oder Konfigurationen zuordnen. Dieselbe Datenbasis nutzt auch die zustandsbasierte Instandhaltung.

Der Weg dorthin ist pyramidal: Zuerst braucht es einen klaren Bezug zur betrieblichen Leistung. Darauf bauen ein vollständiges Inventar mit seinen Abhängigkeiten und eine funktionierende Pflege auf. Automatisierung und KI setzen erst auf dieser Grundlage an. Wer diese Reihenfolge einhält, hat Assetdaten, auf die er sich im Störungsfall ebenso verlassen kann wie bei der nächsten Schwachstellenmeldung.



Cyber Resilienz in der Lieferkette: NIS2 und CRA verändern die Zusammenarbeit im Bahnsektor

Mit NIS2 und dem Cyber Resilience Act reicht die Verantwortung für Cybersicherheit weit in die Lieferkette hinein. Der Beitrag beschreibt, was das für die Zusammenarbeit von Bahnbetreibern und Lieferanten bedeutet und wie Betreiber ihre Lieferanten nach Risiko steuern können.

*Grundlage ist ein Gespräch mit **Martin Heiderich**, Senior Manager Information Security bei Hitachi Rail.*
Autoren:
***Hai Rüdiger**, Managing Consultant, Wavestone*
***Lisa Meyer**, Consultant, Wavestone*

KEY TAKEAWAYS

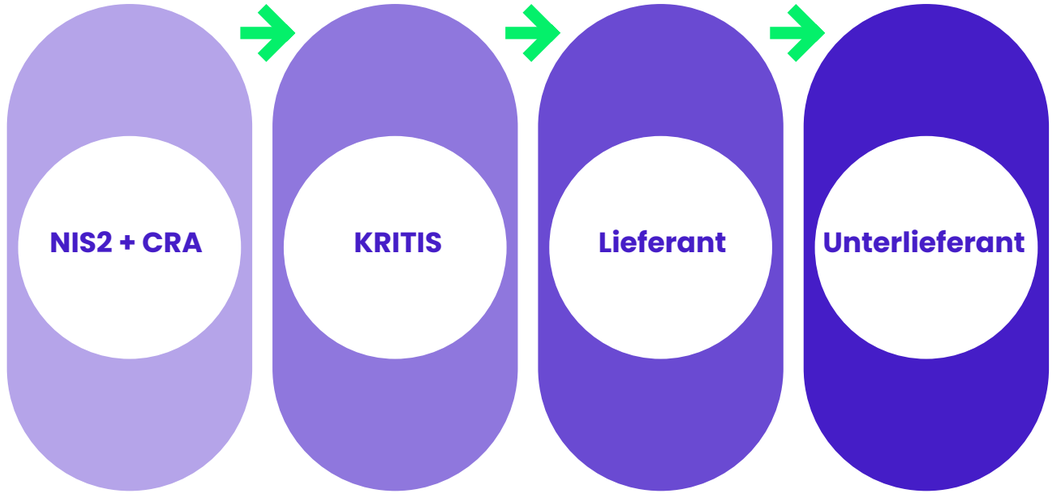
- **Anforderungen wirken entlang der Lieferkette:** NIS2 verpflichtet Betreiber, die Sicherheit ihrer Lieferkette zu steuern. Über Verträge erreichen diese Anforderungen auch Zulieferer, die selbst nicht reguliert sind. Der Cyber Resilience Act (CRA) verpflichtet Hersteller zusätzlich zur Sicherheit ihrer Produkte über den gesamten Supportzeitraum.
- **Die Nachweispflicht überfordert kleine Zulieferer:** Fragebögen mit mehreren hundert Fragen, die jeder Betreiber anders stellt, binden bei Lieferanten Kapazität, ohne die Sicherheit entsprechend zu erhöhen.
- **Anforderungen richten sich nach der Kritikalität:** Lieferanten mit Zugriff auf OT-Systeme, geringer Austauschbarkeit oder einer Rolle im Wiederanlauf brauchen eine intensive Steuerung. Für unkritische Lieferanten genügt ein schlankes Verfahren.
- **Abhängigkeiten bewusst steuern:** Begrenzte Ausweichmöglichkeiten bei Schlüsseltechnologien erfordern langfristige Partnerschaften, Transparenz und klare vertragliche Regelungen.

Lieferanten werden zum Resilienzfaktor kritischer Infrastrukturen

Die Sicherheit eines Bahnunternehmens hängt zunehmend davon ab, wie sicher seine Lieferanten arbeiten.

Angriffe über die Lieferkette haben in den vergangenen Jahren gezeigt, wie ein einziger kompromittierter Dienstleister oder ein manipuliertes Software-Update viele Kunden gleichzeitig treffen kann. Zwei Regelwerke adressieren dieses Risiko von verschiedenen Seiten. NIS2 bzw. das BSIG verpflichtet Betreiber, Risiken in ihrer Lieferkette zu bewerten und zu steuern, bei Produkten ebenso wie bei Dienstleistungen. Der Cyber Resilience Act (CRA) verpflichtet Hersteller von Produkten mit digitalen Elementen zu sicherer Entwicklung, Schwachstellenmanagement und Sicherheitsupdates über einen festgelegten Supportzeitraum. Seit September 2026 gelten erste Meldepflichten für aktiv ausgenutzte Schwachstellen, vollständig anwendbar ist der CRA ab Dezember 2027.

Viele kleinere Zulieferer fallen selbst weder unter NIS2 noch direkt unter die Herstellerpflichten des CRA. Die Anforderungen erreichen sie trotzdem: Der Betreiber gibt sie vertraglich an seine Lieferanten weiter, diese an ihre Unterlieferanten. **Cybersicherheit wird so zu einer gemeinsamen Aufgabe von Betreibern und Lieferanten.**



Besondere Herausforderungen im Bahnsektor

Safety, wenige Hersteller und lange Lebenszyklen erschweren die Umsetzung von NIS2-Anforderungen in der Lieferkette.

Im Bahnsektor treffen regulatorische Anforderungen auf hochverfügbare OT-Systeme, lange Technologiezyklen und eine hohe Abhängigkeit von spezialisierten Lieferanten. Daraus ergeben sich Spannungsfelder, die sich nicht allein durch standardisierte Cybersicherheitsmaßnahmen lösen lassen.

Die folgenden Einblicke basieren auf den Erfahrungen aus Wavestone-Kundenprojekten und auf der Sicht von Heiderich. Er ist seit mehr als zehn Jahren in der Informationssicherheit im Bahnsektor tätig und blickt aus der Rolle des Lieferanten auf die Anforderungen der Betreiber.

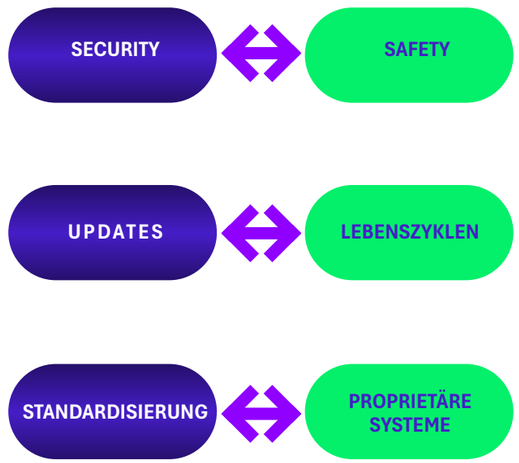
Safety und Verfügbarkeit haben oberste Priorität
Im Bahnbetrieb hat die sichere Betriebsführung höchste Priorität. Zwar gewinnt Cybersicherheit zunehmend an Bedeutung, doch haben Betriebssicherheit und die sichere Verfügbarkeit der Systeme stets Vorrang. Ein Ausfall kritischer Komponenten kann den sicheren Bahnbetrieb unmittelbar beeinträchtigen und im schlimmsten Fall Menschenleben gefährden.

Dadurch entstehen Zielkonflikte zwischen Anforderungen an die Betriebssicherheit (Safety) und an die Cybersicherheit (Security). Informationssicherheitsmaßnahmen erfordern Ressourcen, technische Änderungen oder zusätzliche Prozesse, die sich auf bestehende Betriebs- und Safety-Anforderungen auswirken können. Unternehmen müssen daher stets sowohl Safety als auch Security im Blick behalten und Prioritäten setzen. Nach Beobachtung von Heiderich wird diese Abwägung durch die neuen regulatorischen Anforderungen für manche Unternehmen noch anspruchsvoller. Die Stoßrichtung von NIS2 bewertet er dennoch positiv und als einen wichtigen Schritt zur Verbesserung der Informationssicherheit.

Begrenzte Auswahl an Lieferanten
Viele Bahnsysteme beruhen auf proprietären Technologien, die nur wenige Hersteller anbieten. Ein kurzfristiger Wechsel des Lieferanten ist häufig weder technisch noch wirtschaftlich realisierbar. **Sicherheitsanforderungen können deshalb nicht einfach durch den Austausch eines Lieferanten umgesetzt werden.** Stattdessen gewinnen langfristige Partnerschaften, gemeinsame Sicherheitsstandards und die kontinuierliche Weiterentwicklung bestehender Lieferantenbeziehungen an Bedeutung.



Komplexe und langlebige Systeme
Moderne Bahnsysteme bestehen aus einer Vielzahl miteinander vernetzter IT- und OT-Komponenten. Digitale Stellwerke, Leit- und Sicherungstechnik, Fernwartungslösungen und andere vernetzte Systeme erhöhen die Angriffsfläche und schaffen neue Abhängigkeiten innerhalb der Lieferkette. Diese hohe Komplexität erschwert das Lieferantenrisikomanagement (Third-Party Risk Management; TPRM).



Hinzu kommt, dass viele Systeme über Jahrzehnte betrieben werden. Sicherheitsanforderungen entwickeln sich wesentlich schneller als die zugrunde liegenden Technologien, wodurch Themen wie Schwachstellenmanagement, Sicherheitsupdates und Produktpflege erheblich erschwert werden.

REGULATORISCHE ERWARTUNG	REALITÄT IM BAHNSEKTOR
Schnelle Umsetzung neuer Sicherheitsmaßnahmen	**Lange Lebenszyklen der Systeme**
Austauschbarkeit von Lieferanten	**Herstellerabhängigkeit durch proprietäre Technologien**
Standardisierte Security-Prozesse	**Heterogene IT-/OT-Landschaften**
Hohe Cybersicherheit	**Balance zwischen Security und Safety**
Kontinuierliche Resilienz	**Hohe Abhängigkeit von spezialisierten Lieferanten**

Umsetzung: Zwischen regulatorischem Anspruch und Realität

Mehr Fragebögen bedeuten nicht automatisch mehr Sicherheit

Die regulatorischen Anforderungen aus NIS2 und CRA haben bereits zu einer deutlichen Ausweitung von Lieferantenprüfungen, Sicherheitsnachweisen und Audits geführt.

Für Hersteller kommt mit dem Cyber Resilience Act die Sicherheit ihrer Produkte über deren Lebenszyklus stärker in den Fokus. Im Bahnsektor betrifft das langlebige Systeme und Komponenten, bei denen Schwachstellenmanagement, Sicherheitsupdates und Produktpflege über lange Zeiträume gewährleistet werden müssen. Lieferantenrisikomanagement und Produktsicherheit wachsen damit zunehmend zusammen.

Viele Unternehmen orientieren sich dabei an etablierten Standards wie der ISO/IEC 27001 und verankern entsprechende Anforderungen zunehmend in Verträgen, Ausschreibungen und Lieferantenbewertungen. ISO/IEC 27001 belegt ein funktionierendes Informationssicherheitsmanagementsystem im Unternehmen des Lieferanten. Zudem relevant sind IEC 62443-4-1 (sicherer Entwicklungsprozess beim Hersteller) und IEC 62443-2-4 (Anforderungen an Dienstleister und Integratoren).

Für Lieferanten steigt dabei der Dokumentations- und Nachweisaufwand deutlich. Besonders deutlich zeigt sich dies bei Sicherheitsprüfungen. Heiderich berichtet von sehr umfangreichen Fragebögen, die teilweise mehrere hundert Fragen umfassen. Schon für große Organisationen ist die Bearbeitung solcher Fragebögen mit erheblichem Aufwand verbunden. Für kleinere Lieferanten mit beispielsweise zehn Mitarbeitenden stellt dies häufig eine noch größere Herausforderung dar, da sie dieselben Anforderungen mit deutlich begrenzteren Ressourcen erfüllen müssen.

Neue Anforderungen müssen deshalb so umgesetzt werden, dass sie organisatorisch und wirtschaftlich tragfähig bleiben. Das erfordert Abstimmung mit vielen Beteiligten, denn Lieferantenrisikomanagement betrifft neben der Informationssicherheit auch Einkauf, Vertrieb, Kommunikation, Risikomanagement und Recht. Mit wachsender Abhängigkeit von kritischen Lieferanten gewinnen zudem Business Continuity Management und Krisenmanagement an Gewicht. Entscheidend ist, ob kritische Leistungen bei einem Cybervorfall oder einer Betriebsstörung des Lieferanten aufrechterhalten oder wiederhergestellt werden können.

Das Zielbild einer resilienten Lieferkette

Gemeinsame Verantwortung, risikobasierte Steuerung und kontinuierlicher Informationsaustausch stärken die Resilienz der Lieferkette.

Das Zielbild ist eine Lieferkette, in der Risiken transparent sind, kritische Lieferanten gezielt gesteuert werden und Betreiber sowie Lieferanten ihre Cyber- und Krisenresilienz gemeinsam weiterentwickeln. Ein maximales Kontrollsystem ist dafür weder nötig noch leistbar.

Risikobasierter Ansatz statt Gleichbehandlung

Im Vergabeverfahren und Einkaufsprozess müssen Anbieter und Lieferanten vergleichbarer Produkte oder Leistungen gleichbehandelt werden. Die zunehmenden regulatorischen Anforderungen dürfen jedoch nicht dazu führen, dass über alle Produkt- und Leistungskategorien hinweg identische Anforderungen angesetzt werden. Ein wirksames TPRM orientiert sich an den tatsächlichen Risiken und leitet daraus angemessene Anforderungen für die jeweilige Kategorie ab.

Auch Heiderich sieht die Zukunft in einer stärker risikobasierten Bewertung: Kritische Lieferanten sollten intensiver geprüft werden als solche mit geringerem Einfluss auf den Geschäftsbetrieb.

Mögliche Kriterien für die Kritikalität sind der Zugang zu OT-Systemen, etwa über Fernwartung oder Diagnosegeräte, die Ersetzbarkeit des Lieferanten, die Abhängigkeit kritischer Betriebsleistungen von seinem Produkt, der Umgang mit sensiblen Daten wie Netztopologien und seine Rolle im Wiederanlauf nach einem Vorfall. Daraus ergibt sich die Prüftiefe, von der Selbstauskunft bis zu Audits und gemeinsamen Übungen. Nur so lassen sich Ressourcen gezielt einsetzen und tatsächliche Risiken wirksam adressieren.

Fokus auf tatsächliche Sicherheit

Ein resilientes Unternehmen entsteht nicht allein durch die Erfüllung von Normen und regulatorischen Vorgaben. Normen und Standards liefern zwar einen wichtigen Rahmen, Maßnahmen sollten jedoch nicht nur zu deren Erfüllung umgesetzt werden.

Nach Auffassung von Heiderich sollte zunächst bewertet werden, welche Risiken tatsächlich bestehen und welche Maßnahmen das Unternehmen wirksam schützen. Erst anschließend erfolgt die Einordnung in regulatorische und normative Anforderungen. Normenkonformität bleibt wichtig, das eigentliche Ziel muss jedoch die tatsächliche Erhöhung der Sicherheit sein.

Kommunikation und Sensibilisierung

Technische Maßnahmen allein reichen nicht aus. Damit Anforderungen auch wirken, ist es unerlässlich, dass alle Beteiligten ihre Bedeutung verstehen und sie aktiv unterstützen.

Das gilt sowohl für die eigenen Mitarbeitenden als auch für Lieferanten. Sensibilisierung, praktische Beispiele und ein kontinuierlicher Austausch machen Sicherheitsanforderungen nachvollziehbar und schaffen Akzeptanz. Aus Sicht von Heiderich ist der direkte Dialog dabei häufig wertvoller als der reine Austausch von Mails, Dokumenten oder Fragebögen. Das gilt besonders im Ereignisfall: Kritische Lieferanten

gehören in die Wiederanlaufplanung und in gemeinsame Übungen. **Wer im Ernstfall erstmals mit dem Krisenstab des Herstellers spricht, verliert wertvolle Zeit.**

Sicherheitsinformationen entlang der Kette austauschen

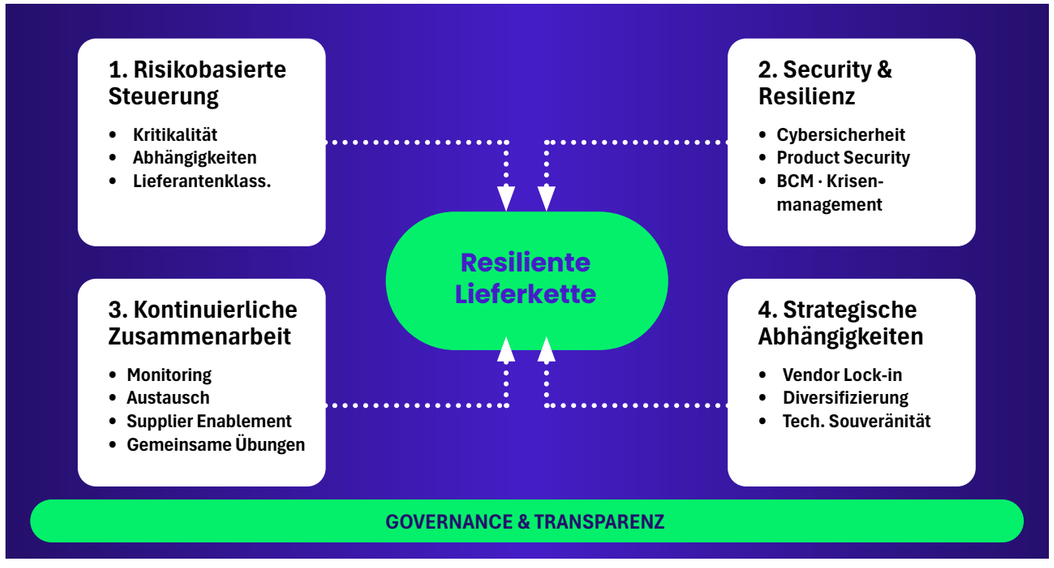
Langfristig wird aus der Bewertung einzelner Lieferanten ein Ansatz für die gesamte Lieferkette. Risiken, Schwachstellen und sicherheitsrelevante Informationen müssen entlang der gesamten Wertschöpfungskette ausgetauscht werden können.

Das Zielbild besteht in einer eng vernetzten Lieferkette, in der Kunden, Hersteller, Dienstleister und Unterlieferanten sicher zusammenarbeiten und Informationen effizient teilen. Perspektivisch können standardisierte und stärker automatisierte Informationsflüsse dazu beitragen, sicherheitsrelevante Informationen effizienter entlang der Lieferkette auszutauschen.

Strategische Abhängigkeiten und europäische Souveränität

Bei proprietären Technologien mit wenigen Anbietern ergeben sich langfristige Abhängigkeiten. Betreiber sollten für jede kritische Abhängigkeit prüfen, welche Optionen sie haben. Wo es technisch möglich ist, können sie diversifizieren, etwa über offene Schnittstellen bei neuen Beschaffungen. Wo ein Wechsel ausgeschlossen ist, sollten sie sich vertraglich absichern, etwa mit langen Supportzusagen, Regelungen für eine Abkündigung und der Hinterlegung von Quellcode bei einem Treuhänder. Wo beides nicht greift, kompensieren sie mit zusätzlichen Schutzmaßnahmen im eigenen Betrieb.

Auf europäischer Ebene sieht NIS2 koordinierte Risikobewertungen kritischer Lieferketten vor. Laut Heiderich ist es darüber hinaus elementar, dass Betreiber, Lieferanten und Unterlieferanten die europäischen Vorgaben zur Informationssicherheit konsequent einhalten. Sicherheitsstandards entlang der gesamten Lieferkette tragen dazu bei, Risiken frühzeitig zu erkennen, die Resilienz zu stärken und regulatorische Anforderungen wirksam umzusetzen.



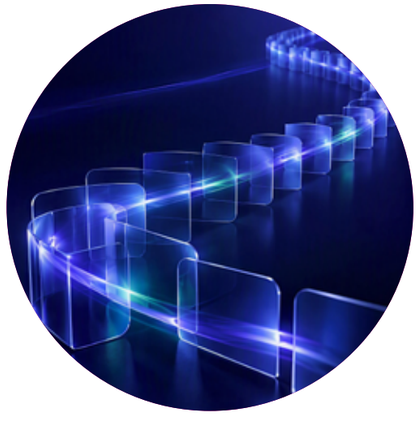
Von der Lieferantenkontrolle zur resilienten Lieferkette: Was Betreiber und Lieferanten jetzt tun sollten

NIS2 und der Cyber Resilience Act verändern das Third-Party Risk Management im Bahnsektor grundlegend. Die Besonderheiten der Branche zeigen dabei, dass eine rein regulatorische Betrachtung nicht ausreicht. Safety-Anforderungen, langlebige Systemlandschaften und die begrenzte Austauschbarkeit spezialisierter Anbieter machen einen pragmatischen, risikobasierten Ansatz erforderlich.

Für Betreiber und Lieferanten ergeben sich daraus vier Handlungsfelder, die dem Zielbild nebenstehenden Grafik entsprechen:

1. Risikobasiert steuern: Nicht jeder Lieferant stellt dasselbe Risiko dar. Kritische Abhängigkeiten müssen transparent gemacht und Lieferanten entsprechend ihrer Bedeutung für Betrieb, Systeme und Lieferfähigkeit klassifiziert werden. Prüfintensität und Sicherheitsanforderungen sollten sich am tatsächlichen Risiko orientieren.

2. Security und Resilienz zusammendenken: Neben den Nachweisen zählt, ob Betreiber und Lieferanten bei einem Vorfall gemeinsam handlungsfähig bleiben. Ihre Anforderungen sollten Betreiber zudem branchenweit abstimmen.



3. Kontinuierlich zusammenarbeiten: Gerade bei spezialisierten und schwer austauschbaren Lieferanten entsteht Resilienz durch langfristige Zusammenarbeit. Sicherheitsanforderungen sollten frühzeitig kommuniziert, Risiken kontinuierlich betrachtet und notwendige Fähigkeiten gemeinsam weiterentwickelt werden. Damit entwickelt sich TPRM von einer punktuellen Lieferantenprüfung zu einem kontinuierlichen Resilienzmanagement entlang der Lieferkette.

4. Strategische Abhängigkeiten absichern: Langfristig gehört dazu auch die Auseinandersetzung mit strategischen Abhängigkeiten. Wo kritische Technologien nur von wenigen Herstellern bezogen werden können, erhöhen Vendor Lock-in und fehlende Alternativen die Verwundbarkeit der Lieferkette. Eine stärkere Diversifizierung von Bezugsquellen und ein konsequenter Blick auf die Einhaltung europäischer Vorgaben können dazu beitragen, Abhängigkeiten zu reduzieren, Risiken entlang der Lieferkette zu minimieren und deren Resilienz nachhaltig zu stärken.

Ein Unternehmen ist nur so resilient wie seine Lieferanten und Dienstleister. Wer seine kritischen Abhängigkeiten kennt, die Risiken seiner Partner bewertet und Sicherheitsanforderungen vertraglich festlegt und nachhält, macht die eigene Lieferkette beherrschbar.

KI-gestütztes Security Monitoring im Bahnsektor: Erst das Fundament, dann die Automatisierung

Das Gesetz verlangt von Betreibern kritischer Bahninfrastruktur, dass sie Cyberangriffe frühzeitig erkennen. Doch vielerorts fehlen die entsprechenden Fachkräfte. Kann KI im Security Operations Center (SOC) diese Lücke schließen? Der Beitrag ordnet ein, was heute realistisch möglich ist und mit welchen Maßnahmen Bahnunternehmen am besten beginnen sollten.

Grundlage ist ein Gespräch mit einem Cyber Defence Experten aus der Bahnindustrie
*Autor: **Fabian Böhm**, Managing Consultant, Wavestone*

KEY TAKEAWAYS

- **Erweiterung, kein Ersatz:** KI-gestütztes Security Monitoring erweitert das Security Operations Center bei Erkennung, Triage und Reaktion und ersetzt weder Analysten noch betriebliches Kontextwissen.
- **Erst das Fundament:** In IT/OT-Umgebungen mit Legacy-Systemen und Verfügbarkeitsdruck zahlt sich KI erst aus, wenn Asset-Transparenz, grundlegendes Security Monitoring und Incident Response bereits vorhanden sind.
- **Verhaltensbasierte Erkennung:** Verhaltensbasierte Analyse und UEBA erkennen in deterministischen OT-Netzen Anomalien und Identitätsmissbrauch, die regelbasierte Systeme übersehen. Voraussetzung ist eine saubere Datenbasis.
- **Der Mensch entscheidet:** Ohne „Human in the Loop", Nachvollziehbarkeit und Governance produziert KI-gestütztes Security Monitoring nur zusätzliche (Fehl-)Alarme. In der Bahn-OT erkennt und empfiehlt die KI, entscheiden müssen Menschen.
- **Gesetzliche Pflicht zur Angriffserkennung:** Betreiber kritischer Anlagen sind gesetzlich zum Einsatz von Systemen zur Angriffserkennung verpflichtet (§ 31 BSIG). KI-gestütztes Monitoring muss deshalb auditierbar und kontrollierbar bleiben.
- **KI ist selbst Angriffsfläche:** Assistenten verarbeiten große Mengen Logdaten, die Angreifer beeinflussen können. Agenten mit Zugriff auf Sicherheitswerkzeuge brauchen deshalb minimale Rechte und lückenlose Protokollierung.

Security Monitoring ist für Bahnbetreiber Pflicht

KI-gestütztes Security Monitoring stärkt das Bahn-SOC nur als Erweiterung reifer Security Operations.

Angriffe auf kritische Infrastrukturen werden professioneller und treffen zunehmend auch betriebsnahe Umgebungen. Fällt dort ein System aus, wirkt sich das unmittelbar auf Fahrbetrieb und Mobilität aus.

Für Betreiber kritischer Anlagen ist der Einsatz von Systemen zur Angriffserkennung gesetzlich vorgeschrieben (§ 31 BSIG). Sie müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Das BSI hat dazu eine Orientierungshilfe veröffentlicht. Mit NIS2 kommen kurze Meldefristen hinzu: eine Frühwarnung nach 24 Stunden und eine erste Bewertung nach 72 Stunden. Beides setzt voraus, dass Vorfälle auch in der OT zeitnah erkannt und eingeordnet werden.

Gleichzeitig fehlt Personal. Ein SOC, das rund um die Uhr IT und OT überwacht und dabei sowohl Stellwerksprotokolle als auch Ereignisse aus der Unternehmens-IT einordnen kann, ist mit dem verfügbaren Fachpersonal kaum zu besetzen. **Hier liegt das stärkste Argument für KI-Unterstützung: Sie lenkt die knappe Expertise auf die Fälle, die tatsächlich eine Bewertung benötigen.**

KI-gestütztes Security Monitoring verspricht eine schnellere Erkennung und eine bessere Priorisierung. Dieser Nutzen stellt sich jedoch nicht automatisch ein. Ausschlaggebend sind der Reifegrad, die Datenqualität, die Governance und die klare Verbindung von automatisierter Analyse und menschlicher Bewertung.

Regelbasiertes Monitoring stößt in der Bahn-OT an Grenzen

Erkennungstechnologie ist selten das Problem. Die Probleme liegen woanders: Alarme in einer Menge, die niemand bewältigen kann, sowie Lücken in den Daten und Ereignisse, die sich ohne OT-Kontext nicht bewerten lassen.

Bahninfrastrukturen verbinden moderne IT mit langlebiger OT. Leit- und Sicherungstechnik, Stellwerke und Energieversorgung laufen teils über Jahrzehnte, nutzen proprietäre Protokolle und müssen hochverfügbar bleiben. Standardmaßnahmen wie Patching, invasive Sensorik oder vollständige EDR-Anbindung sind deshalb nur eingeschränkt umsetzbar.

In dieser Umgebung stößt eine regelbasierte Erkennung an ihre Grenzen. Signaturen und statische Regeln erzeugen viele Meldungen mit begrenzter Aussagekraft. Kritische Vorfälle gehen im Rauschen unter, während Analysten immer mehr Zeit für die Bewertung von Alerts aufwenden müssen. Gerade schleichende oder unbekannte Angriffe bleiben so zu lange unentdeckt.

Hier liegt der erste greifbare Mehrwert von KI: verhaltensbasierte Analyse. KI-Modelle lernen das Normalverhalten von Systemen, Nutzern und Prozessen und melden Abweichungen frühzeitig. In

größtenteils deterministischen OT-Netzen ist das besonders wirksam, weil ungewöhnliche Kommunikation dort häufig direkt auf Störung oder Angriff hinweist. UEBA ergänzt dies, indem Identitätsmissbrauch sichtbar wird, den klassische Signaturen oft übersehen.

Das Normalverhalten im Bahnbetrieb ist allerdings nicht statisch. Beim Fahrplanwechsel, bei Baustellen, im Störfallbetrieb oder während Wartungsfenstern kommt es zu legitimen Abweichungen. Wenn das Monitoring davon nichts weiß, meldet es genau diese Abweichungen. Zuverlässig wird die Anomalieerkennung in der Bahn-OT deshalb erst, wenn sie Daten aus der Betriebs- und Wartungsplanung erhält: geplante Arbeiten, freigegebene Fernwartungssitzungen, aktuelle Betriebszustände. **Diese Daten anzubinden ist aufwendiger als die Sensorik selbst und wird in Projekten regelmäßig unterschätzt.**

Für die Praxis bedeutet das: KI zuerst dort einsetzen, wo verhaltensbasierte Erkennung den größten Hebel hat, also in OT-Segmenten mit stabilen Kommunikationsmustern und bei der Erkennung kompromittierter Identitäten. Die bestehenden Regeln bleiben daneben in Kraft.

Wann KI menschliche Analysten entlastet

KI wirkt im Security Monitoring nur mit „Human in the Loop". Sie entfaltet erst mit erklärbaren Ergebnissen und klarer Governance ihre volle Wirkung.

Über die Erkennung hinaus unterstützt KI vor allem Triage, Analyse und Reaktion. Sie korreliert Ereignisse, priorisiert Alerts und bereitet Entscheidungen vor. Dadurch verschiebt sich die Rolle der Analysten von repetitiver Bearbeitung hin zu Bewertung, Koordination und Freigabe.



Der Nutzen bleibt jedoch an Bedingungen geknüpft. KI-Ergebnisse müssen nachvollziehbar sein, Daten müssen klassifiziert und geschützt werden, und kritische Entscheidungen dürfen nicht vollständig automatisiert werden. Gerade im regulierten Bahnbetrieb müssen Detektion und Reaktion auditierbar bleiben.

Wirksame Implementierungen folgen deshalb konsequent dem Prinzip „Human in the Loop". KI übernimmt Voranalyse, Priorisierung und Handlungsvorschläge; die finale Bewertung bleibt bei qualifizierten Analysten. So werden Fehlentscheidungen, Halluzinationen und Fehlpriorisierungen begrenzt.

Dabei sind drei Arten von KI zu unterscheiden, deren Reife und Risiken deutlich voneinander abweichen:

- Auf Machine Learning (ML) basierende Anomalieerkennung in OT-Monitoring und UEBA ist seit Jahren im Einsatz. Ihre Ergebnisse lassen sich auf konkrete Abweichungen von einer Baseline zurückführen.
- LLM-Assistenten fassen Alerts zusammen, korrelieren Ereignisse und schlagen nächste Schritte vor. Sie verkürzen die Triage, können aber plausibel klingende Fehlinterpretationen liefern.
- Agentische Systeme führen Abfragen, Anreicherungen und Gegenmaßnahmen selbstständig aus. Sie haben das größte Effizienzpotenzial und brauchen die engsten Leitplanken.

KI ist dabei selbst eine neue Angriffsfläche. LLM-Assistenten verarbeiten Logdaten, in die ein Angreifer gezielt Anweisungen einschleusen kann (Prompt Injection). Agenten greifen mit privilegierten Rechten auf Sicherheitswerkzeuge zu und sind damit ein attraktives Ziel. KI-Komponenten brauchen deshalb dieselbe Sicherheitsbetrachtung wie jedes andere privilegierte System: minimale Berechtigungen, vollständige Protokollierung ihrer Aktionen, getrennte Freigaben für lesende und verändernde Zugriffe und regelmäßige Tests auf Manipulierbarkeit.

In der Bahn-OT sollte KI daher auf absehbare Zeit Auffälligkeiten erkennen, Informationen anreichern und Handlungsempfehlungen geben, aber nicht selbst eingreifen. Das wichtigste Argument hierfür ist das „Fail-safe"-Prinzip der Leit- und Sicherungstechnik: Wird eine Komponente automatisch isoliert, kann das Signale auf Halt setzen und den Zugverkehr stoppen. **Eine automatische Abwehrreaktion würde dann selbst den Betrieb stören.** Über Eingriffe entscheidet deshalb weiterhin der Mensch, in Abstimmung mit der Betriebszentrale. In der Unternehmens-IT lassen sich klar definierte Reaktionen dagegen automatisieren, etwa das Sperren eines kompromittierten Kontos.

Ein weiterer Erfolgsfaktor ist die Reife der Betriebsbasis. Asset-Transparenz, vollständiges Logging auch in der OT, definierte Incident-Response-Prozesse und klare Verantwortlichkeiten sind die Voraussetzung dafür, dass KI sinnvolle Ergebnisse liefert. Wer KI auf ein unreifes Fundament setzt, automatisiert bestehende Lücken.

Architektur und Sourcing für ein KI-fähiges SOC

Ob KI im SOC funktioniert, entscheidet sich weniger am Modell als an drei Grundlagen: Architektur, Datenhoheit und Sourcing.

Der Nutzen von KI ergibt sich aus dem Zusammenspiel von Architektur, Betriebsmodell und Governance. Einzelne Funktionen bringen wenig. Eine tragfähige SOC-Architektur verbindet SIEM, OT-spezifisches Monitoring und eine KI-Analyseschicht. OT-Daten verlassen die betrieblichen Zonen dabei nur über kontrollierte Übergänge.

Der Nutzen agentischer Ansätze hängt stark vom Reifegrad der Erkennungsfähigkeiten eines Betreibers ab. Betreiber, die noch Herausforderungen bei den grundlegenden Aspekten wie Assetmanagement, Logging, Incident Response oder Betriebsprozessen haben, profitieren meist mehr von der Konsolidierung ihrer bestehenden Werkzeuge und Prozesse als von komplexen KI-Architekturen. Agenten und Automatisierung lohnen sich erst auf einer stabilen Betriebsbasis.

Mit zunehmendem Reifegrad wächst der Bedarf an spezialisierten Funktionen. Standardplattformen bilden dann das Fundament, spezifische Analyse-, Automatisierungs- oder Integrationsfunktionen werden schrittweise ergänzt. Eine modulare Architektur hält diese Funktionen austauschbar und vermeidet langfristige Abhängigkeiten von einzelnen Herstellern.

Auch das Sourcing muss bewusst entschieden werden. Die zentrale Frage ist, welche Daten an Modelle des Herstellers oder eines Cloud-Anbieters fließen dürfen. Netzwerktopologien, Konfigurationen und Kommunikationsmuster von Stellwerken sind für Angreifer wertvoll. Viele Betreiber werden deshalb einen hybriden Weg wählen: Die Analyse sensibler OT-Daten bleibt im eigenen Rechenzentrum oder in einer souveränen Umgebung, Cloud-Dienste nutzen nur freigegebene, bereinigte Daten.

Regulatorisch kommt der EU AI Act hinzu. Reine Analyse- und Assistenzfunktionen im SOC dürften nicht als Hochrisiko-KI gelten. Anders kann es aussehen, wenn KI automatisiert in betriebliche Systeme eingreift. Dann sollte die Einstufung im Einzelfall geklärt werden. Das spricht zusätzlich dafür, in der Bahn-OT bei Empfehlungen zu bleiben und Eingriffe dem Menschen zu überlassen.



Für die Praxis heißt das: zuerst ein steuerbares Fundament aufbauen, herstellerneutral entscheiden und kritisches Domänenwissen im eigenen Haus halten. Das Wissen über Bahnbetrieb und OT-Kontext ist die Grundlage jeder Bewertung, die eine KI vorbereitet.

Der Einstieg folgt einer klaren Reihenfolge

Wer zuerst Daten, Kontext und Zuständigkeiten klärt, holt aus KI im SOC am meisten heraus.

Für Bahnbetreiber zählt vor allem, ungeplante Betriebsunterbrechungen zu vermeiden. Messbar wird der Nutzen von KI über eine Ausgangsbasis, die vor der Einführung festgelegt wird: die mittlere Zeit bis zur Erkennung (MTTD) und bis zur Eindämmung (MTTR), die Fehlalarmquote und der Anteil automatisch vorqualifizierter Alerts.

Agentische Systeme verändern die Arbeitsweise im SOC: Analysten steuern Abfragen und Anreicherungen zunehmend über KI-Agenten und bedienen weniger Werkzeuge einzeln. Der Mehrwert liegt in der engen Zusammenarbeit von Fachexperten und Agenten entlang des Analyse- und Reaktionsprozesses.

Für den Einstieg empfehlen wir drei pragmatische Schritte:

1. Reifegrad ehrlich bewerten: Asset-Transparenz, Logging auch in der OT, Incident Response und 24/7-Betrieb prüfen, bevor Budget in KI fließt. Erkannte Lücken zuerst schließen.

2. KI mit dem größten Hebel einsetzen: Mit verhaltensbasierter Analyse in stabilen OT-Netzen beginnen, gekoppelt an die Betriebs- und Wartungsplanung, und mit der Erkennung von Identitätsmissbrauch bei Fernwartung und Dienstkonten. LLM-Assistenten folgen für die Triage, agentische Funktionen zunächst nur in der IT.

3. Architektur und Sourcing strategisch verankern: Herstellerneutral entscheiden, ein hybrides Modell mit gewahrter Datenhoheit wählen und kritisches Kontextwissen im eigenen Haus halten.

Wer so vorgeht, kann die gesetzliche Pflicht zur Angriffserkennung auch mit knappem Personal erfüllen und Vorfälle früher entdecken.

In der Bahn-OT erkennt und empfiehlt die KI, entscheiden müssen Menschen.

BCM auf die Schiene bringen: Pläne, die im Ereignisfall funktionieren

Bahnunternehmen verfügen über Richtlinien, Business-Impact-Analysen und Notfallpläne. Ob diese im Ereignisfall weiterhelfen, zeigt sich erst, wenn Betrieb, IT und Krisenstab mit ihnen arbeiten müssen. Der Beitrag beschreibt, wie ein Business Continuity Management (BCM) aussieht, das im Bahnbetrieb tatsächlich genutzt wird.

*Grundlage ist ein Gespräch mit **Tim Neubert**, Bereichsreferent Unternehmenssicherheit bei der Rheinbahn AG, der seine Erfahrung aus dem Personenverkehr einbringt.*
*Autoren: **Johannes Oschinsky**, Manager, Wavestone, **Ann-Sophie Hauke**, Manager, Wavestone*

KEY TAKEAWAYS

- **Wirksamkeit statt Dokumentation:** Wirksam wird ein BCMS im Bahn- und Personenverkehr erst, wenn es Betriebsleistungen auch in Störungs- und Krisensituationen kontrolliert aufrechterhält. Dokumentation allein reicht dafür nicht.
- **Abhängigkeiten kennen:** Der Reifegrad eines BCMS zeigt sich daran, wie gut zeitkritische Geschäftsprozesse, kritische Ressourcen und ihre Abhängigkeiten organisationsweit bekannt sind und gesteuert werden.
- **Disziplinen verzahnen:** Cybervorfälle erfordern ein enges Zusammenspiel von Betrieb, IT, Informationssicherheit, Krisenmanagement und Kommunikation. Diese Disziplinen arbeiten auf der präventiven sowie der reaktiven Achse zusammen, also bei der Vorbereitung ebenso wie im Ereignisfall.
- **Gemeinsam mit dem Betrieb:** BCM muss gemeinsam mit dem Betrieb entwickelt werden. Nur dann sind Pläne, Prozesse, Verfahren und Entscheidungswege im Ereignisfall tatsächlich nutzbar.
- **Regulatorischer Nachweisdruck:** NIS2, das KRITIS-Dachgesetz und die Notfallvorkehrungen im Sicherheitsmanagementsystem nach Eisenbahnrecht erhöhen den Druck, die Wirksamkeit des BCM nachzuweisen und es in ein integriertes Resilienzmanagement einzubinden.

Warum Business Continuity im Bahnbetrieb eine operative Aufgabe ist

Im Bahnsektor sichert BCM Verfügbarkeit und Führungsfähigkeit. Als reine Dokumentationsaufgabe verfehlt es diesen Zweck.

Im Bahnbetrieb greifen Fahrbetrieb, Betriebszentralen, Stellwerke, Fahrzeuge, Werkstätten, Energieversorgung, Fahrgastinformation, Vertriebssysteme und externe Dienstleister eng ineinander. Fällt eines dieser Elemente aus, bleibt die Wirkung selten lokal begrenzt. Sie setzt sich entlang von Umläufen, Instandhaltung, Kundenkommunikation und Ersatzverkehren fort. BCM ist in diesem Umfeld weniger eine formale Ergänzung zur Governance als vielmehr eine operative Kernfähigkeit.

Mit der Digitalisierung wächst diese Bedeutung weiter. IT/OT-Konvergenz, vernetzte Betriebs- und Geschäftsprozesse, externe Plattformen und digitale Kundenschnittstellen vergrößern die Angriffs- und Ausfallflächen. Cybervorfälle sind dabei ein wesentlicher Treiber, aber nicht der einzige. Auch technische Ausfälle, Extremwetterereignisse, Lieferantenausfälle, Personalausfälle oder physische Sicherheitsereignisse können die Betriebsfähigkeit erheblich beeinträchtigen. Entscheidend ist deshalb, ob kritische Leistungen bei einem Ausfall kontrolliert fortgeführt oder geordnet wieder angefahren werden können. Ob das BCMS dokumentiert ist, beantwortet diese Frage nicht.



BCM aus dem Elfenbeinturm in den Betrieb

Die größte Lücke liegt zwischen der formalen BCM-Logik und dem, was im Betrieb tatsächlich genutzt wird.

In unserer Beratungspraxis sehen wir häufig BCM-Systeme, die aus einer formalen Perspektive aufgebaut wurden: mit Richtlinien, Rollenmodellen, Business-Impact-Analysen, Planvorlagen, Kennzahlen und Review-Zyklen. Diese Elemente sind notwendig. Sie reichen aber nicht aus, wenn sie nicht an die Realität des Bahnbetriebs anschließen und gelebt werden. **Im Ereignisfall zählt, ob ein Plan genutzt werden kann.** Wie vollständig er ist, spielt dann kaum eine Rolle. BCM muss deshalb gemeinsam mit dem Betrieb entwickelt werden.

Neubert bestätigt das aus seiner Erfahrung im Personenverkehr. Er beschreibt den Status quo als historisch stark auf den Kernprozess Fahrgastbeförderung fokussiert. Das betriebliche Notfallmanagement sei vielfach auf diesen Kernprozess und seine technischen Komponenten ausgerichtet, müsse aber *„auf die gesamtorganisatorische Ebene angehoben“* werden. Unterstützungsprozesse, die für die Verfügbarkeit des Betriebs wesentlich sind, würden bislang häufig nicht mit derselben Konsequenz betrachtet. Dazu gehören etwa die Personal- und Fahrzeugdisposition, die Ersatzteil- und Werkstattlogistik, die Beschaffung von Ersatzverkehren und IT-Dienste wie Identitäts- und Kommunikationssysteme.

Wirksames BCM im Bahnsektor betrachtet deshalb auch die Prozesse, Ressourcen und Entscheidungsstrukturen, die den Betrieb unter Störbedingungen absichern. Mindestbetriebszustände, Eskalationswege, Wiederanlaufprioritäten und Ressourcenabhängigkeiten müssen so beschrieben sein, dass sie im Ereignisfall das Handeln anleiten.

Ein Mindestbetriebszustand im Personenverkehr kann etwa ein Grundangebot auf den Hauptachsen in festem Takt sein, ergänzt durch Ersatzverkehre auf Nebenstrecken und eine Fahrgastinformation, die auch manuell funktioniert. Für diesen Zustand wird festgelegt, welche Fahrzeuge, welches Personal und welche Systeme mindestens verfügbar sein müssen.

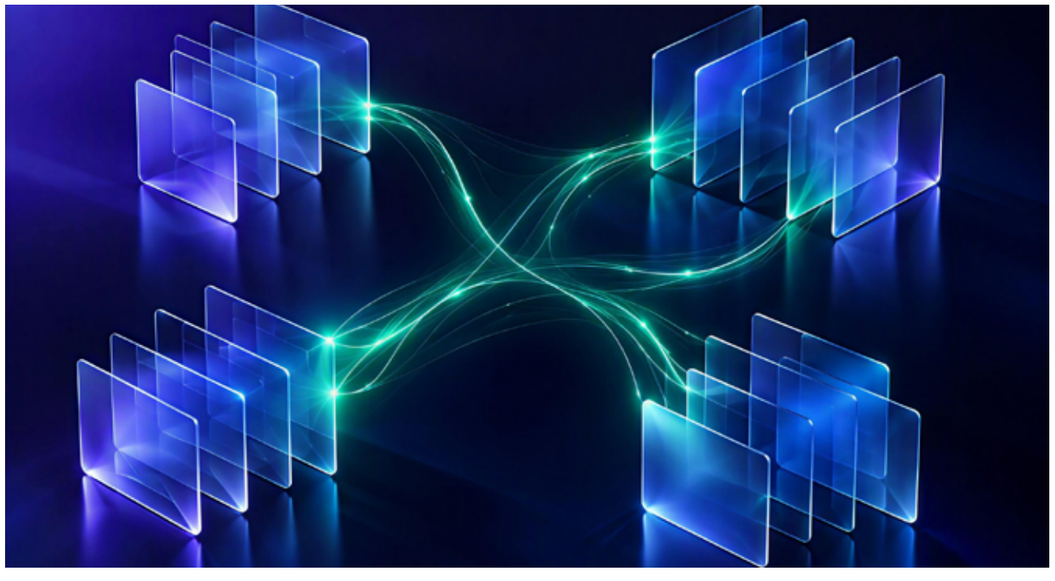
All-Hazard: Pläne nach Wirkungen ordnen

BCM ordnet Ereignisse nach ihrer Wirkung auf kritische Leistungen und führt gleiche Reaktionen zusammen.

Business Continuity lässt sich im Bahnsektor nicht auf Cyber Recovery reduzieren. Ihr Wert liegt gerade darin, unterschiedliche Auslöser über ihre Auswirkungen auf kritische Leistungen vergleichbar zu machen. Ob Ransomware, Dienstleisterausfall, Energieproblem, Extremwetterereignis, Personalausfall, Sabotage oder Lieferkettenproblem: Für den Betrieb stellen sich häufig dieselben Fragen nach Mindestleistung, zwingend benötigten Ressourcen, Ersatzverfahren, Priorisierung, Kommunikation und Anbindung an den Krisenstab. Der All-Hazard-Ansatz ist damit die Voraussetzung dafür, dass Pläne bei ganz unterschiedlichen Ursachen angewendet werden können.

In der Praxis scheitert diese Logik häufig an überdifferenzierten Szenarienkatalogen. Neubert verweist auf Gefahrenabwehrpläne mit *„über 400 Szenarien“* und macht deutlich, worin das Problem liegt: In vielen Fällen sei *„der Handlungsstrang […] immer der gleiche“*. Aus seiner Sicht muss Notfallplanung deshalb höher abstrahieren, Kategorien bilden und identische Reaktionsmuster zusammenführen. Das deckt sich mit unserer Erfahrung: Wer die Ursachen immer weiter verästelt, erhöht den Dokumentationsaufwand. Wer nach Wirkungen und Reaktionsmustern strukturiert, erhöht hingegen die Chance, dass Pläne tatsächlich aktiviert werden.

Nicht jeder Ausfall braucht deshalb einen eigenen Plan. Jede kritische Wirkungslage braucht aber eine vorbereitete Reaktion. Das reduziert die Komplexität und erhöht die Wahrscheinlichkeit, dass Pläne unter Zeitdruck tatsächlich wirksam angewendet werden.



Business Impact beginnt bei Leistungen

Eine Business-Impact-Analyse (BIA) orientiert sich an Leistungen, Wertströmen und Abhängigkeiten. Organigramme sind dafür der falsche Ausgangspunkt.

Ein häufiger Schwachpunkt im BCM ist die Orientierung an Organisationseinheiten. Im Bahnbetrieb führt das schnell zu blinden Flecken. Entscheidend ist, welche Verkehrs-, Infrastruktur- und Unterstützungsleistungen unterbrechungskritisch sind, wie lange ihr Ausfall tragbar ist und welche Ressourcen ihren Wiederanlauf bestimmen. Dafür gibt es etablierte Kennzahlen: die maximal tolerierbare Ausfallzeit (MTA), die Wiederanlaufzeit (RTO) und den maximal tolerierbaren Datenverlust (RPO). Die BIA wird deshalb entlang betrieblicher Wertströme aufgebaut, von Betriebsführung und Fahrbetrieb über Infrastruktur, Fahrgastinformation, Vertrieb, Instandhaltung und Energieversorgung bis zu Kommunikation und zentralen Steuerungsfunktionen.

Damit diese Analyse steuerungsfähig wird, braucht BCM ein klares Bild der Prozesse und ihrer Abhängigkeiten. Anwendungen, OT-Komponenten, Betriebsressourcen, Lieferanten, Standorte und Verantwortlichkeiten müssen in ihrer Wechselwirkung sichtbar sein. Ohne dieses Verständnis bleiben Business-Continuity-Pläne (BC-Pläne) abstrakt. Neubert formuliert diesen Punkt sehr klar: *„Allein ein BCM ohne Prozesse ist für mich kein BCM."* Ebenso deutlich verweist er darauf, dass eine BIA ohne Geschäftsprozesse ihren Zweck verfehlt.

Aus unserer Sicht liegt hier eine zentrale Reifegradfrage für den Sektor. Nur wenn zeitkritische Leistungen und ihre Abhängigkeiten durchgängig transparent sind, lassen sich Mindestbetriebszustände definieren, realistische Ersatzverfahren planen und Wiederanlaufpfade priorisieren. Dies markiert den Unterschied zwischen einem dokumentierten BCM und einem BCM, das im Ernstfall handlungsfähig macht.

Aktivierbare Pläne schlagen perfekte Dokumente

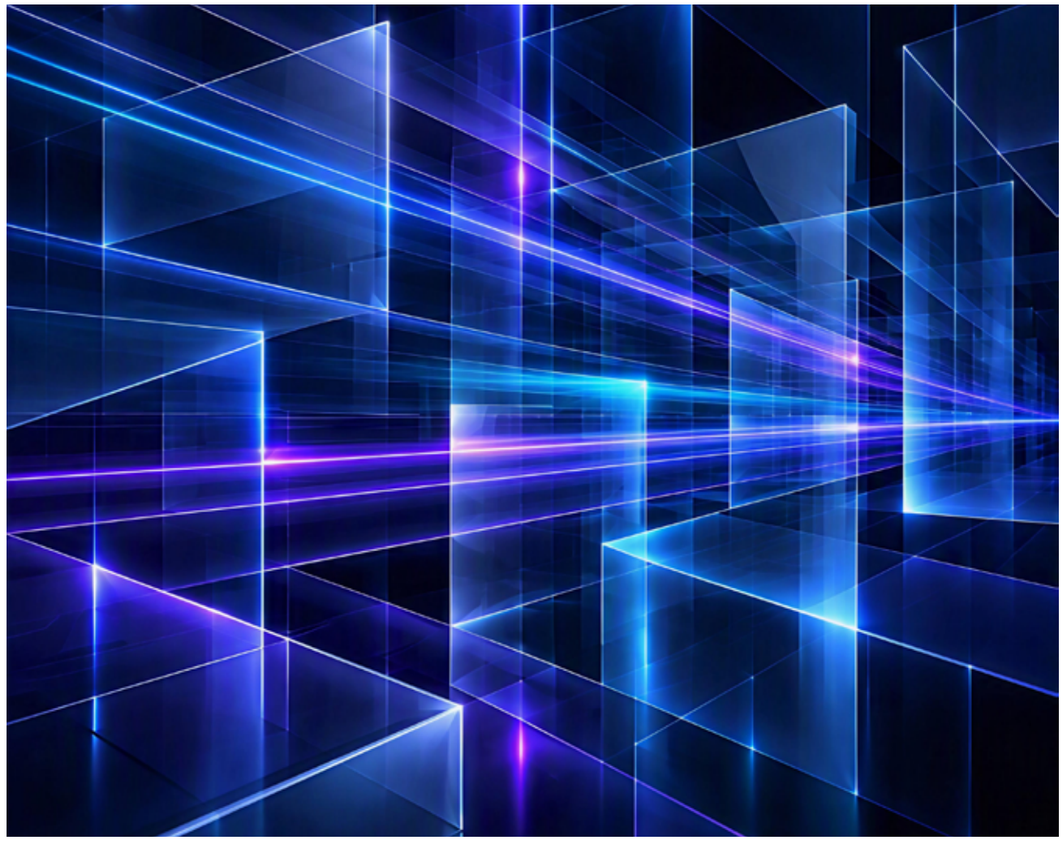
Ein BC-Plan ist dann gut, wenn er unter Zeitdruck funktioniert und von den operativ Verantwortlichen sofort genutzt werden kann.

BCM wird im Ereignisfall daran gemessen, ob es sich aktivieren lässt. Ein Plan braucht klare Auslöser, eindeutige Rollen, kurze Entscheidungswege, priorisierte Maßnahmen, erprobte Kommunikationswege und realistische Wiederanlaufannahmen. Vor allem muss er so geschrieben sein, dass neben BCM-Fachleuten auch Betriebsverantwortliche, Leitstellen, IT, Informationssicherheit, Kommunikation, Corporate Security und Krisenmanagement damit arbeiten können.

Gerade im Bahnsektor ist das entscheidend, weil Ereignisse selten eindimensional verlaufen. Ein Cyberangriff kann gleichzeitig Fahrgastinformation, Disposition, externe Kommunikation und regulatorische Meldepflichten betreffen. Ein Dienstleisterausfall kann auf Instandhaltung und Fahrzeugverfügbarkeit zurückwirken. Ein IT-Ausfall kann manuelle Ersatzverfahren im Betrieb erforderlich machen. Pläne müssen deshalb über die Grenzen der Fachbereiche hinweg funktionieren.

Für Cyberlagen kommen einige Anforderungen hinzu. BC-Pläne müssen offline verfügbar sein, denn im Intranet sind sie bei einem Ransomware-Angriff nicht erreichbar. Manuelle Ersatzverfahren dürfen nicht selbst an der ausgefallenen IT hängen. Backups werden offline oder unveränderlich vorgehalten. Der Wiederanlauf folgt einer festgelegten Reihenfolge, die in der Regel mit den Identitätsdiensten beginnt, weil ohne sie kaum ein anderes System nutzbar ist.

Übungen sind der wichtigste Nachweis, ob BCM wirkt. Sie zeigen, ob Rollen greifen, Eskalationen funktionieren und Annahmen tragfähig sind. Besonders aussagekräftig sind Übungen, die bewusst Schnittstellen belasten: kombinierte IT/OT-Lagen, Ausfälle mit Wirkung auf Fahrgastinformation oder manuelle Ersatzverfahren im Betrieb. **BCM darf im Bahnsektor nicht erst im Ernstfall zum ersten Mal genutzt werden.**



Raus aus den Silos

Die zentrale Aufgabe der nächsten Jahre ist es, Betrieb, Risikomanagement, Sicherheit und Kontinuität zusammenzuführen.

Wirksames BCM im Bahnbetrieb ist Schnittstellenmanagement. Es verbindet Perspektiven, die im Alltag unterschiedlichen Logiken folgen: Betrieb denkt in Verfügbarkeit, Disposition und Sicherheit; IT in Services und Wiederherstellung; Informationssicherheit in Schutzbedarf und Incident Response; Corporate Security in physischer Lage und Schutzmaßnahmen; Krisenmanagement in Führung, Lagebild und Kommunikation. BCM bezieht diese Perspektiven aufeinander, ohne sie zu vereinheitlichen.

Darin liegt der Wert eines integrierten Resilienzmanagements. Neubert beschreibt dies als übergeordnetes Zielbild und bringt den zentralen Befund auf den Punkt: *„Wir denken noch in Silos und wir müssen da raus."* Seine zweite Beobachtung ist für Transformationsvorhaben ebenso relevant: Ein solches Zielbild lässt sich mit Methodik allein nicht aufbauen, es braucht Verständigung. Sein Leitsatz dafür lautet: *„Kommunikation, Kommunikation, Kommunikation."* In der Praxis heißt das: Betrieb, IT, Informationssicherheit und Krisenmanagement erarbeiten die BIA gemeinsam, nutzen im Ereignisfall dasselbe Lagebildformat und üben am selben Szenario.

Aus Wavestone-Sicht ist das der wichtigste Schritt für den Sektor. Regulierung, Digitalisierung und Bedrohungslage erhöhen den Druck, die Wirksamkeit des BCM nachzuweisen. Ein BCM, das gemeinsam mit dem Betrieb entwickelt und regelmäßig geübt wird, hilft im Ereignisfall, den Zugverkehr kontrolliert weiterzuführen.

> **Allein ein BCM ohne Prozesse ist für mich kein BCM.**
>
> *Tim Neubert, Bereichsreferent Unternehmenssicherheit bei der Rheinbahn AG*



Krisenmanagement im Bahnsektor: Von gemeinsamen Begriffen zur Handlungsfähigkeit

Bahnunternehmen verfügen über hoch spezialisierte Fähigkeiten für Betrieb, Technik und Unternehmenssteuerung. In einer komplexen Situation zählt, ob diese Bereiche dieselbe Lage vor Augen haben und unter Zeitdruck gemeinsam entscheiden können. Der Beitrag beschreibt, wie Bahnunternehmen dafür eine gemeinsame Sprache für Störung, Notfall und Krise schaffen und ihre Krisenorganisation einüben.

*Grundlage ist ein Gespräch mit **Thomas Theisejans**, Chief Expert IT/OT-Notfallmanagement der Deutschen Bahn AG.*

Autor: **Daniel Nussbaumer**, *Associate Partner, Wavestone*

KEY TAKEAWAYS

- **Schutzziele zuerst:** Wie ein Ereignis eskaliert, richtet sich nach seiner Wirkung auf die Leistungen, die das Unternehmen unter allen Umständen erbringen muss. Diese Schutzziele gehören vor jede Krisendefinition.
- **Eskalationsstufen für alle Lagen:** In vielen Bahnkonzernen sind Notfall- und Krisenstrukturen dezentral gewachsen. Gemeinsame Eskalationsstufen von Störung, Notfall und Krise mit messbaren Eskalationskriterien, etwa auf Basis des BSI-Standards 200-4, verbinden sie. Auch Cyberlagen sind in denselben Eskalationsstufen enthalten.
- **Das Lagebild trennt Wissen und Annahmen:** Ein Lagebild ist ein fortlaufender Arbeitsprozess. In Cyberlagen muss es zudem damit umgehen, dass die Daten aus den eigenen Systemen möglicherweise manipuliert sind.
- **Handlungsfähig durch gemeinsames Training:** Pläne allein reichen nicht. Handlungsfähig wird eine Organisation durch gemeinsame Ausbildung nach einheitlichen Standards und durch Übungen, die auch den Ausfall von Schlüsselpersonen durchspielen.
- **Der Vorstand setzt den Rahmen und hält sich daran:** Die Geschäftsleitung verantwortet die Krisenfähigkeit und trifft die strategischen Leitentscheidungen. Im Ereignisfall greift sie nicht am Krisenstab vorbei in die operative Steuerung ein.

Eine Krise beginnt mit der Frage, was geschützt werden muss

Maßstab für die Eskalation ist die Wirkung eines Ereignisses auf die Leistungen, die geschützt werden müssen.

Bahnunternehmen tragen Verantwortung für die Sicherheit von Reisenden und Personal und für eine Mobilitätsleistung, von der große Teile von Wirtschaft und Gesellschaft abhängen. Ob ein Ereignis als Störung, Notfall oder Krise einzuordnen ist, hängt deshalb vor allem von seiner Wirkung auf diese Leistungen ab. Die technische Ursache ist dafür zweitrangig.

Theisejans leitet die Krisenorganisation konsequent aus diesem Auftrag ab: *„Bevor eine Organisation ihre Krise definiert, muss sie wissen, wofür sie existiert und was sie unter allen Umständen schützen muss.“* Aus diesen Schutzzielen ergeben sich die Übergänge zwischen den Eskalationsstufen. Derselbe technische Auslöser kann lokal beherrschbar bleiben oder strategische Bedeutung gewinnen. Das hängt davon ab, wann er eintritt, welche Abhängigkeiten er berührt und wie die Öffentlichkeit ihn wahrnimmt.

Für den Bahnsektor ergibt sich daraus eine klare Perspektive: Krisenmanagement sichert die Fähigkeit, Mobilität auch unter außergewöhnlichen Bedingungen verantwortbar aufrechtzuerhalten. Welche Tragweite dieser Auftrag hat, macht Theisejans am Beispiel der Pandemie deutlich: *„In der Coronazeit war nahezu alles heruntergefahren, aber die Bahn fuhr weiter. Genau darin zeigt sich Daseinsvorsorge: Mobilität aufrechtzuerhalten, obwohl sich auf eine Lage dieser Größenordnung niemand vollständig vorbereiten konnte.“*

Schutzziele sollten daher konkret genug sein, um im Ereignisfall Entscheidungen zu tragen. Ein allgemeines Bekenntnis zur Daseinsvorsorge reicht dafür nicht. Bewährt hat sich die Festlegung eines Mindestangebots, also der Verbindungen und Leistungen, die auch in einer schweren Lage aufrechterhalten werden sollen. Daran lassen sich Prioritäten und Eskalationsschwellen ausrichten.



Gemeinsame Begriffe schaffen gemeinsame Entscheidungen

Eine Organisation kann nur dann koordiniert eskalieren, wenn alle Bereiche dieselben Eskalationsstufen anlegen.

In großen Bahnorganisationen entstehen Notfall- und Krisenstrukturen oft dezentral. Fachbereiche, Regionen und Tochtergesellschaften entwickeln eigene Begriffe und Verfahren. Im Alltag funktioniert das. **In einer bereichsübergreifenden Lage führt es dazu, dass dasselbe Ereignis an einer Stelle als Störung und an einer anderen als Notfall gilt.**

Ansatzpunkt ist für Theisejans deshalb das gemeinsame Vokabular: ***„Eine wirksame Krisenorganisation beginnt mit einer gemeinsamen Definition von Störung, Notfall und Krise."***

Die Definitionen müssen von den regulatorischen Vorgaben bis in die operativen Einheiten anschlussfähig sein. Regionale und fachliche Einheiten können ihre Organisation weiterhin selbst ausgestalten, solange sie dieselben Eskalationskriterien anwenden. Eine naheliegende Grundlage ist der BSI-Standard 200-4. Er definiert die Eskalationsstufen und beschreibt Business Continuity Management einschließlich Krisenmanagement. Ergänzend bietet ISO 22361 einen Rahmen für das Krisenmanagement.

Das gilt besonders für Cybervorfälle. Ein technischer Incident berührt schnell den Betrieb, die Kommunikation und die gesetzlichen Meldepflichten. Einheitliche Schwellenwerte und Meldewege führen die Fachperspektiven zu einer gemeinsamen Bewertung. Klare Begriffe ermöglichen dabei eine frühzeitige Einordnung der Lage und ein koordiniertes Vorgehen.



Vom Organigramm zum beweglichen Gesamtsystem

Die Krisenorganisation verbindet strategische, taktische und operative Ebene und bindet die bestehende Notfallorganisation der Bahn ein.

Diese Verbindung erstreckt sich nach Theisejans über mehrere Ebenen. Die strategische Ebene richtet die Organisation an ihren Schutzzielen aus und trifft die Leitentscheidungen. Die taktische Ebene übersetzt diese Vorgaben in Risikomanagement und Krisenvorsorge. Auf der operativen Ebene handeln die Einsatzkräfte unmittelbar an Anlagen, Systemen und Betriebsprozessen.

Das Modell muss auch dann funktionieren, wenn Personen ausfallen oder Zuständigkeiten sich ändern. Den Anspruch formuliert Theisejans so: *„Ich brauche stabiles, breit aufgestelltes Wissen, idealerweise ergänzt durch tiefgehende Experten."* Jede Rolle im Stab braucht deshalb Stellvertretungen, die mit ihr geübt haben. Benachbarte Rollen müssen genug voneinander verstehen, um eine Lücke vorübergehend zu überbrücken. So entwickelt sich aus einer starren Pyramide ein bewegliches Gesamtsystem.
Für die operative Steuerung im Ereignisfall bündelt ein zentrales Crisis Management Team das Lagebild und bereitet Entscheidungen vor. Fachliche Zellen, etwa für Betrieb, IT, OT und Kommunikation, bewerten die Lage in ihrer Domäne und steuern dort die Maßnahmen. Die Fachverantwortung bleibt in den Zellen, das Crisis Management Team koordiniert.

Das Lagebild ist ein fortlaufender Arbeitsprozess

Ein Lagebild trennt gesicherte Fakten von Annahmen und zeigt, welche Entscheidungen anstehen.

Für Theisejans ist das Lagebild ein Arbeitsmittel, das sich ständig ändert: *„Das Lagebild ist ein Moving Target, das sich mit Situation, Zeit und Entwicklung verändert."* Ein brauchbares Lagebild unterscheidet deshalb gesicherte Fakten, Annahmen, offene Fragen und anstehende Entscheidungen mit ihrem Zeitfenster. Es zeigt, welche Leistungen bereits beeinträchtigt sind und welche als Nächstes gefährdet sind.

Cyberlagen stellen das Lagebild vor zusätzliche Anforderungen. Solange unklar ist, welche Systeme kompromittiert sind, können auch Monitoring, Logs und Berichte aus diesen Systemen falsch sein. Forensische Erkenntnisse kommen oft erst nach Tagen, während sich betriebliche Auswirkungen und externe Anfragen stündlich ändern. Die Frühwarnung an behördliche Stellen ist oft innerhalb von 24 Stunden fällig, häufig bevor die Lage verstanden ist. Zudem können Cyberkrisen Wochen dauern. Der Stab benötigt daher einen Schichtbetrieb, der die Handlungsfähigkeit über den gesamten Zeitraum hinweg sicherstellt.

Früherkennung erweitert diese Logik nach außen. Monitoring und Open Source Intelligence können Hinweise liefern, bevor Auswirkungen im eigenen Betrieb sichtbar werden. Wie schnell sich die Bewertung ändern kann, veranschaulicht Theisejans an einem betrieblichen Beispiel: *„Ein Trafobrand kann zunächst nur eine Störung sein. Durch regionale Auswirkungen und mediale Präsenz wird daraus mit einem Schlag eine Krise."* Hinweise sollten deshalb früh geprüft werden, anhand fester Schwellenwerte und unterhalb des Vorstandskrisenstabs. Der Zweck ist Zeitgewinn. Eine vorschnelle Eskalation würde den Stab dagegen mit Lagen belasten, die auf operativer Ebene beherrschbar sind.

Standardisierung wird durch Training wirksam

Pläne geben Orientierung. Handlungsfähig macht eine Organisation erst die gemeinsame Übung.

Den Wert gemeinsamer Ausbildung sieht Theisejans bei Behörden und Organisationen mit Sicherheitsaufgaben (BOS) sowie militärischen Organisationen belegt. Menschen aus verschiedenen Einheiten arbeiten dort zusammen, weil sie dieselben Begriffe und Grundverfahren kennen. Große Bahnunternehmen können dieses Prinzip mit konzernweiten Standards für Lagebilder, Meldungen, Entscheidungen und Stabsarbeit übertragen.

Standards regeln dabei die Übergabepunkte zwischen den Fachbereichen, deren Methoden bleiben unberührt. Vier Fragen strukturieren jeden Übergabepunkt: Welche Information wird benötigt? Wer bewertet sie? Wer entscheidet? Wie werden Maßnahmen nachgehalten? Klar definierte Schnittstellenfunktionen übersetzen Fachwissen in eine Sprache, mit der der Krisenstab arbeiten kann.

Übungen zeigen, wo die Übergaben in der Praxis haken. Sie sollten realistische Belastungen enthalten, zum Beispiel den Ausfall von Schlüsselpersonen, nicht verfügbare IT-Systeme im Krisenstab selbst oder eine Lage, die über mehrere Tage und Schichtwechsel läuft. Die Erkenntnisse fließen anschließend in Standards und Ausbildung zurück. Die Logik dahinter bringt Theisejans auf den Punkt: „Prozesse verbessert man in Friedenszeiten. Im laufenden Krisenfall braucht es Verlässlichkeit statt spontaner Neuerfindung."



Führung braucht Mandat und Disziplin

Die Geschäftsleitung verantwortet die Krisenfähigkeit. Im Ereignisfall stärkt sie die vorbereitete Organisation, indem sie sich an deren Rollen hält.

Die Rolle der Führung ist für Theisejans eine zentrale Governance-Frage. Eigentümer, Vorstand oder Geschäftsführung setzen qualifizierte Verantwortliche ein, geben ein klares Mandat und greifen auch unbequeme Erkenntnisse auf. Im Ereignisfall halten sie sich an die Rollen im Krisenstab und greifen nicht an ihm vorbei in operative Entscheidungen ein. Führung verantwortet den Rahmen und die strategischen Leitentscheidungen, die operative Steuerung folgt den vorbereiteten Stabsprozessen.

Am stärksten wird ein Krisenstab daher oft von oben belastet. Wenn Vorstandsmitglieder im Ereignisfall direkt Fachbereiche ansteuern oder eigene Lagebilder anfordern, laufen parallele Entscheidungswege, und der Stab verliert den Überblick. Diese Disziplin sollte die Geschäftsleitung deshalb selbst mitüben.

Besondere Bedeutung hat die Kommunikation. Sie arbeitet unmittelbar am Lagebild und wird von professionellen Kommunikationsfunktionen verantwortet. Im Bahnsektor hat sie mehrere Adressatenkreise: Beschäftigte, Behörden und Öffentlichkeit sowie die Fahrgäste. Die Fahrgastinformation ist dabei ein eigener, zeitkritischer Kanal, der selbst an IT-Systemen hängt. In einer Cyberlage kann auch die interne Kommunikation betroffen sein. Sind E-Mail oder Collaboration-Plattformen kompromittiert, braucht der Stab vorbereitete Ausweichkanäle mit vorab verteilten Kontaktlisten.

Was Bahnunternehmen jetzt anders machen sollten

Fünf konkrete Schritte zu einer Krisenorganisation, die auch unter Veränderung funktioniert.

Für Bahnunternehmen ergeben sich daraus fünf Schritte:

- Schutzziele und Mindestangebot festlegen: Sie bilden den Maßstab für Eskalation und Priorisierung.
- Konzernweite Eskalationsstufen einführen: Sie gelten für alle Lagen, auch für Cybervorfälle, und haben messbare Kriterien für den Übergang von Störung zu Notfall zu Krise.
- Notfallorganisation, Cybersecurity und Konzernkrisenstab verzahnen: mit gemeinsamen Übergabepunkten und einem gemeinsamen Lagebildformat.
- Stabsrollen gemeinsam ausbilden und mit Stellvertretungen üben: auch in Szenarien, in denen die eigene IT nicht verfügbar ist.
- Die Rolle der Geschäftsleitung für Krisenlagen festlegen und mitüben.

Eine Krise hält sich nicht an Organigramme. Handlungsfähig bleibt die Organisation, die ihre Zuständigkeiten über Bereichsgrenzen hinweg vorbereitet und geübt hat, bevor es darauf ankommt.

Workforce Readiness im Bahnsektor: Der blinde Fleck der Operational Resilience

Bahnunternehmen investieren in Cybersecurity, Business Continuity Management (BCM) und Krisenmanagement. Im Ernstfall tragen Menschen diese Fähigkeiten: in der Betriebszentrale, im Stellwerk, in der Werkstatt und im Krisenstab. Ob genügend von ihnen im Ernstfall tatsächlich verfügbar sind, prüfen die wenigsten Unternehmen. Der Beitrag beschreibt, warum „Workforce Readiness" weit mehr ist als ein HR-Thema und warum Bahnunternehmen die personelle Einsatzbereitschaft künftig systematisch in BCM, Krisenmanagement und Resilienzplanung aufnehmen sollten.

*Grundlage ist ein Gespräch mit **Nico Gramenz**, Gründer und Geschäftsführer von takeKONTROL.*
*Autor: **Martin Wölfel**, Senior Manager, Wavestone*

KEY TAKEAWAYS

- **Menschen sind die unausgesprochene Voraussetzung:** BCM-Pläne, Rückfallebenen und Krisenstäbe setzen voraus, dass genügend qualifizierte Menschen verfügbar sind. Ob diese Annahme in einer regionalen Krise hält, prüfen die wenigsten Bahnunternehmen.
- **Rückfallebenen brauchen mehr Personal:** Manuelle Ersatzverfahren sind personalintensiver als der Regelbetrieb. Gerade wenn weniger Menschen verfügbar sind, braucht der degradierte Betrieb mehr von ihnen, und zwar mit Qualifikationen, die an bestimmte Anlagen und Strecken gebunden sind.
- **Der Engpass liegt oft im privaten Umfeld:** Wer nicht weiß, ob die eigene Familie versorgt ist, steht im Ereignisfall nur eingeschränkt zur Verfügung. Persönliche Vorsorge der Beschäftigten ist deshalb Teil der Unternehmensresilienz.
- **Planen auf Ebene der Rollen:** Ein Lagebild zur personellen Einsatzbereitschaft muss mit dem Datenschutz und dem Betriebsrat vereinbar sein. Die Planung erfolgt auf Ebene von Rollen und aggregierten Zahlen. Angaben zur persönlichen Situation bleiben freiwillig.
- **Reservisten & Ehrenamtliche in Hilfsorganisationen fallen doppelt ins Gewicht:** In einer sicherheitspolitischen Krise wird die Bahn für militärische Transporte gebraucht, während Reservisten unter den Beschäftigten einberufen werden können und Mitglieder aus Hilfsorganisationen ebenfalls gebunden sind. Diese Konstellation sollte vorab geklärt sein.

Resilienz setzt voraus, dass die Menschen da sind

Die Verfügbarkeit von Systemen wird genau analysiert. Die Verfügbarkeit der Beschäftigten wird meist stillschweigend vorausgesetzt.

Der Bahnbetrieb ist durch enge Abhängigkeiten zwischen Fahrbetrieb, Leitstellen, Stellwerken, Instandhaltung, Energieversorgung, Kommunikation und externen Dienstleistern geprägt. Cyberangriffe, IT/OT-Störungen, Extremwetter oder hybride Bedrohungen treffen deshalb selten nur ein einzelnes System. Sie wirken in den Betrieb hinein, wo Menschen unter Druck entscheiden und handeln.

Viele Resilienzprogramme adressieren diese Lage über BCM, Notfallpläne, Wiederanlaufkonzepte und technische Redundanzen. Das ist richtig, reicht aber nicht aus. Denn jedes dieser Konzepte setzt voraus, dass ausreichend qualifizierte Menschen verfügbar sind. Gramenz bringt diesen Zusammenhang im Gespräch bewusst schlicht auf den Punkt: *„Wenn du ein Unternehmen retten willst, brauchst du halt Menschen dafür."*
In der Praxis wird genau das selten geprüft. Eine Business-Impact-Analyse (BIA) nach BSI-Standard 200-4 oder ISO 22301 erfasst zwar Personal als Ressource: Sie fragt, wie viele Personen mit welcher Qualifikation eine kritische Leistung braucht. Offen bleibt meist, ob diese Personen in einer regionalen Krise zur Arbeit kommen können, weil sie selbst betroffen sind, Angehörige versorgen müssen oder den Arbeitsort nicht erreichen.

Aus Wavestone-Sicht liegt hier ein zentraler blinder Fleck der Operational Resilience: Organisationen analysieren die Verfügbarkeit von Systemen, Standorten und Lieferketten sehr genau, behandeln die Verfügbarkeit der Beschäftigten aber oft als implizite Annahme. Für den Bahnsektor ist das riskant, denn im Ernstfall sind es Menschen, welche die Notfallpläne oft unter schwierigen Bedingungen umsetzen.



Rückfallebenen brauchen mehr Menschen

Im degradierten Betrieb steigt der Personalbedarf, während die Verfügbarkeit sinkt.

Fallen digitale Systeme aus, greift der Bahnbetrieb auf manuelle Verfahren zurück: Zugleitbetrieb, schriftliche Befehle, zusätzlich besetzte Stellwerke, manuelle Fahrgastinformation. Diese Rückfallebenen sind erprobt. Sie brauchen aber deutlich mehr Personal als der Regelbetrieb, und das wird in der Planung oft übersehen.

Zugleich lässt sich Personal im Bahnbetrieb nicht beliebig austauschen. Fahrdienstleiter sind für bestimmte Stellwerkstypen befähigt, Triebfahrzeugführer brauchen Strecken- und Baureihenkenntnis, und in Instandhaltung sowie Leit- und Sicherungstechnik sind Qualifikationen oft an einzelne Anlagen gebunden. Hinzu kommen Arbeitszeitgrenzen: Längere Schichten sind nach dem Arbeitszeitgesetz nur in engen Ausnahmen zulässig, etwa in Notfällen. Bei sicherheitsrelevanten Tätigkeiten ist Übermüdung zudem selbst ein Risiko. **Eine mehrtägige Lage lässt sich deshalb nicht allein mit Überstunden überbrücken.**

Jeder Mindestbetriebszustand im BCM sollte daher mit dem Personal hinterlegt sein, das er tatsächlich braucht, nach Rollen, Qualifikationen und Schichten. Erst dann zeigt sich, ob er mit realistisch verfügbaren Beschäftigten über mehrere Tage durchzuhalten ist.



Der Engpass liegt oft im privaten Umfeld

Beschäftigte sind in einer Krise auch Eltern, Angehörige oder selbst Betroffene.

In einer Krise handeln Mitarbeitende nicht ausschließlich in ihrer beruflichen Rolle. Sie sind zugleich Eltern, Angehörige, Pflegepersonen, Reservisten, Mitglieder von Hilfsorganisationen oder selbst von einer regionalen Lage betroffen. Fallen Kommunikation, Kinderbetreuung oder Verkehrswege aus, klären sie zuerst, ob ihr eigenes Umfeld versorgt ist.

Im Gespräch beschreibt Gramenz diesen Mechanismus als harte Voraussetzung für Einsatzbereitschaft. Wer nicht weiß, ob die Kinder betreut sind oder wie Angehörige erreicht werden können, steht der Organisation im Ereignisfall nur eingeschränkt zur Verfügung. Persönliche Vorbereitung gehört deshalb zur Unternehmensresilienz.

Für Bahnunternehmen wiegt das besonders schwer, weil sich viele kritische Tätigkeiten weder aus dem Homeoffice erledigen noch verschieben lassen. Wer Leitstellen besetzt, Fahrzeuge instand hält, Störungen disponiert oder manuelle Ersatzverfahren organisiert, muss zur richtigen Zeit vor Ort handlungsfähig sein. Für die Workforce Readiness ergeben sich daraus drei operative Fragen: Welche Menschen brauchen wir wirklich? Was könnte ihre Verfügbarkeit beeinträchtigen? Und was können wir vor der Krise tun, damit sie ihre Rolle wahrnehmen können?

Zwei Gruppen verdienen besondere Aufmerksamkeit: Reservisten der Bundeswehr sowie Angehörige von Hilfsorganisationen. Im Spannungs- oder Verteidigungsfall steigt der Transportbedarf, während Reservisten unter den Beschäftigten einberufen werden können. Die Bundeswehr bezieht Unternehmen der kritischen Infrastruktur in ihre Planung ein. Gleiches gilt für ehrenamtliche Funktionen in Hilfsorganisationen wie dem Deutschen Roten Kreuz. Für Beschäftigte in kritischen Funktionen können Arbeitgeber eine Unabkömmlichstellung beantragen. Dafür muss vorab bekannt sein, welche Funktionen unverzichtbar sind und wer sie ausfüllt. Wichtig ist, dass Arbeitgeber und Beschäftigte sich hierzu austauschen.



Ein Lagebild über Menschen, das keine Überwachung ist

Im Rahmen des BCM beantwortet die Business-Impact-Analyse, wie viele personelle Ressourcen benötigt werden. Workforce Readiness beantwortet die Frage, wer im Krisenfall tatsächlich verfügbar ist.

Gramenz beschreibt die Ausgangslage im Gespräch als *„kompletten Blindflug“*: Oft ist nicht bekannt, wer in einer außergewöhnlichen Lage verfügbar wäre. Die Personaleinsatzplanung für den Normalbetrieb beantwortet diese Frage nicht. Gebraucht wird ein Verständnis dafür, welche Rollen in einer Krise kritisch sind, wo personelle Engpässe drohen und was die Verfügbarkeit einschränken kann.

Viele dieser Faktoren sind sensibel: familiäre Verpflichtungen, lange Pendelwege, ehrenamtliche Funktionen, Reservistenstatus, gesundheitliche Belastungsgrenzen. Die Erhebung solcher Angaben unterliegt dem Beschäftigtendatenschutz, für Gesundheitsdaten gelten besonders strenge Regeln. Werden technische Systeme zur Erfassung eingesetzt, hat der Betriebsrat ein Mitbestimmungsrecht. Ein belastbares Lagebild setzt deshalb bei den Rollen an und nicht bei einzelnen Personen:

Rollen und Qualifikationen: Welche Rollen sind für den Mindestbetrieb unverzichtbar? Wie viele qualifizierte Personen gibt es je Rolle, und wie viele Stellvertretungen sind eingeübt?

Freiwillige Selbstauskunft: Beschäftigte in kritischen Rollen können angeben, ob sie in bestimmten Szenarien voraussichtlich verfügbar wären. Die Angabe ist freiwillig, Gründe müssen sie nicht nennen.

Aggregierte Auswertung: Die Planung arbeitet mit Quoten je Rolle und Standort. Einzelne Personen sind darin nicht erkennbar.

Betriebsvereinbarung: Zweck, Umfang und Grenzen der Erhebung werden gemeinsam mit dem Betriebsrat festgelegt.

Damit verändert sich die Perspektive im BCM. Zur Frage, welche Prozesse wiederhergestellt werden müssen, kommt eine zweite: Welche Menschen tragen diese Prozesse, und unter welchen Bedingungen bleiben sie handlungsfähig? Idealerweise sollte dabei der Betriebsrat von Anfang an beteiligt werden. **Ein Lagebild, das Beschäftigte als Kontrolle empfinden, liefert keine ehrlichen Angaben.** Wird der Zweck offen erklärt und mit konkreter Unterstützung verbunden, steigt die Bereitschaft, realistisch Auskunft zu geben.

Persönliche Vorbereitung ermöglichen

Das Unternehmen kann die private Vorsorge nicht übernehmen. Es kann sie aber leichter machen.

Im Gespräch mit Gramenz werden drei Dimensionen persönlicher Vorbereitung deutlich: Zur praktischen Vorsorge gehören Absprachen mit der Familie, vereinbarte Treffpunkte, wichtige Dokumente und Vorräte, um einige Tage ohne gewohnte Versorgung auszukommen. Mentale Vorbereitung heißt, sich mit möglichen Szenarien auseinanderzusetzen, bevor sie eintreten. Körperliche Belastbarkeit wird wichtig, wenn Menschen über längere Zeit unter Hitze, Schlafmangel oder hoher Unsicherheit arbeiten müssen.

Es geht darum, Beschäftigten die Vorbereitung zu erleichtern, ohne zusätzliche Erwartungen an sie zu stellen. Gramenz formuliert dafür eine klare Haltung: *„Die Wahrheit ist den Menschen zumutbar.“* Wer Krisenfähigkeit ernst nimmt, spricht offen über mögliche Szenarien und bietet konkrete Hilfen an.

Solche Hilfen können Informationen zur privaten Notfallvorsorge sein, etwa auf Basis des Ratgebers des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK). Dazu kommen vorbereitete Wege, über die Beschäftigte im Ereignisfall ihre Angehörigen erreichen und Informationen vom Arbeitgeber erhalten, sowie Regelungen zur Kinderbetreuung im Krisenfall, wie es sie während der Pandemie für Beschäftigte in kritischen Berufen gab. In Übungen lernen Beschäftigte zudem ihre Rolle im degradierten Betrieb kennen.

Was Bahnunternehmen jetzt tun sollten

Personelle Einsatzbereitschaft gehört in BCM und Krisenmanagement. Ein separates HR-Programm reicht dafür nicht.

Bahnunternehmen sollten zunächst gemeinsam klären, welche personellen Fähigkeiten für den Betrieb unter Störbedingungen unverzichtbar sind. Beteiligt sind Betrieb, IT und OT, Informationssicherheit, Corporate Security, BCM, Krisenmanagement, HR und Mitbestimmung, mit einem Mandat des Vorstands.

Kritische Rollen erfassen: Für jeden Mindestbetriebszustand wird festgelegt, welche Rollen, Qualifikationen und Schichten er braucht, einschließlich des Mehrbedarfs der Rückfallebenen.

Das Lagebild mit dem Betriebsrat vereinbaren: Zweck, Freiwilligkeit und Aggregation werden in einer Betriebsvereinbarung geregelt.

Die BIA um die realistische Verfügbarkeit ergänzen: Übungen laufen bewusst mit reduzierter Besetzung, um zu prüfen, ob die Planung trägt.

Die Frage von Reservisten und Hilfsorganisationen klären: Beschäftigte in kritischen Funktionen werden identifiziert, das Verfahren zur Unabkömmlichstellung wird vorbereitet.

Beschäftigte bei der Vorsorge unterstützen: mit Informationen, Kommunikationswegen und Regelungen für die Betreuung von Angehörigen.

Systeme lassen sich redundant auslegen, Beschäftigte nicht. Bahnunternehmen, die ihre personelle Einsatzbereitschaft kennen und die Vorsorge ihrer Beschäftigten unterstützen, können ihre Rückfallebenen im Ernstfall auch tatsächlich besetzen.

Kontakt:



Martin Wölfel
Delivery Lead Security & Resilience
LinkedIn ↗



Isabella Geis
Delivery Lead Transport & Infrastructure
LinkedIn ↗

Autoren:

Bernhard Barth
Associate Partner, München
IT/OT-Konvergenz im Bahnsektor
LinkedIn ↗

Fabian Böhm
Managing Consultant, München
KI-gestütztes Security Monitoring im Bahnsektor
LinkedIn ↗

Ann-Sophie Hauke
Manager, Köln
BCM auf die Schiene bringen
LinkedIn ↗

Lisa Meyer
Consultant, Köln
Cyber Resilienz in der Lieferkette
LinkedIn ↗

Daniel Nussbaumer
Associate Partner, Zürich
Krisenmanagement im Bahnsektor
LinkedIn ↗

Marc-André Ohk
Managing Consultant, Köln
NIS2 im Bahnsektor
LinkedIn ↗

Johannes Oschinsky
Manager, Berlin
BCM auf die Schiene bringen
LinkedIn ↗

Hai Rüdiger
Managing Consultant, Frankfurt
Cyber Resilienz in der Lieferkette
LinkedIn ↗

Jonathan Schläger
Partner, Köln
NIS2 im Bahnsektor
LinkedIn ↗

Markus Wendl
Manager, Köln
Assetmanagement im Bahnsektor
LinkedIn ↗

Martin Wölfel
Senior Manager, Berlin
Hybride Bedrohung im KRITIS-Sektor Transport und Verkehr
Workforce Readiness im Bahnsektor
LinkedIn ↗

ÜBER WAVESTONE

Aus den Anfängen der digitalen Innovation heraus hat sich Wavestone zu einer der führenden Beratungen an der Schnittstelle von Business und Technologie entwickelt. Das Unternehmen unterstützt weltweit führende Organisationen dabei, neue Arbeitsweisen zu skalieren, ihre Abläufe zu transformieren und ihre Geschäftsmodelle im Zeitalter der KI neu zu denken.

Mit 6.000 Mitarbeitenden in Europa und Nordamerika vereint Wavestone Business-, Transformations- und Technologiekompetenzen, um maßgeschneiderte End-to-End-Beratungsleistungen zu erbringen. Künstliche Intelligenz ist dabei fester Bestandteil der Kompetenzen und Leistungsangebote des Unternehmens. So wird ihr Potenzial für Kunden zu greifbarem und nachhaltigem Mehrwert.

Wavestone ist an der Euronext Paris notiert und als Great Place to Work® zertifiziert.
wavestone.com



WAVESTONE