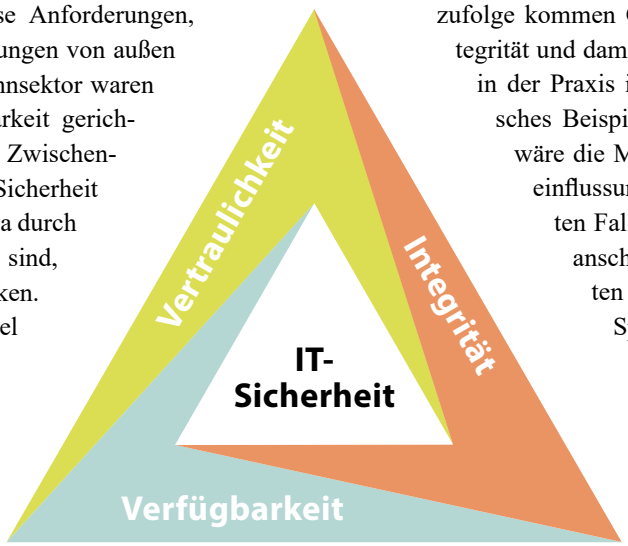
# BAHN-IT MUSS WACHSENDEN GEFAHREN TROTZEN

*Barbara Feldmann*

Wie eine Reihe von kritischen Systemübergriffen in den vergangenen Jahren und Monaten gezeigt hat, ist das Thema IT-Sicherheit für den Bahnsektor akuter denn je. Beim Schutz digitaler Infrastrukturen geht es um mehr als das Einrichten einer Firewall: Cybersecurity, der Schutz operationaler Technologien und Infrastrukturen, die Manipulationssicherheit sensibler Daten oder auch die Neuausrichtung des Sicherheitsverständnisses im Unternehmen spiegeln den Facettenreichtum wider, den ein übergreifendes IT-Sicherheitskonzept berücksichtigen muss. Mit diesem Beitrag startet der *bahn manager* eine fünfteilige Artikelserie, in der die einzelnen Aspekte von IT-Sicherheit im System Schiene beleuchtet werden.

Vertraulichkeit, Integrität, Verfügbarkeit – die Zielsetzung jeder IT-Sicherheitsstrategie lässt sich im Wesentlichen auf diese drei Grundfesten zurückführen. Erfüllen Hardware, Softwaresysteme und Prozesse diese Anforderungen, sind sie gegen Angriffe und Einwirkungen von außen geschützt. Bisherige Angriffe im Bahnsektor waren primär auf das Schutzziel Verfügbarkeit gerichtet. Dennoch gehören auch kritische Zwischenfälle, bei denen die funktionale Sicherheit (FuSi) und damit Leib und Leben etwa durch Stellwerksmanipulationen gefährdet sind, zum Spektrum der möglichen Risiken. In diesem Fall greift das Schutzziel der Integrität, das vom Bundesamt für Informationsschutz in der Informationssicherheit (BSI) als „durchgängiges Funktionieren von IT-Systemen sowie eine Vollständigkeit und Richtigkeit von Daten und Informationen“ definiert ist. Der Aspekt der Vertraulichkeit, das dritte Schutzziel jeder IT-Sicherheitsstrategie, tangiert den Bereich der Datensicherheit. Hierunter fallen unter anderem der Schutz von sensiblen Daten wie etwa Fahrgastinformationen oder auch die manipulationssichere Dokumentation von Zugsteuerungsprozessen.




## PRIMÄRES ZIEL: VERFÜGBARKEIT

Das Eisenbahnsystem arbeitet nach dem Prinzip, dass in einem unsicheren oder nicht definierten Betriebszustand unverzüglich der Stillstand hergestellt wird. Etwaige Angriffe können dadurch zwar einen beträchtlichen (volks-)wirtschaftlichen Schaden nach sich ziehen, sie sind jedoch zunächst einmal nicht lebensgefährlich. Dr. Lukas Iffländer, Referent Cybersecurity beim Deutschen Zentrum für Schienenverkehrsforschung beim Eisenbahn-Bundesamt (DZSF), gibt jedoch zu bedenken: „Sollten solche Angriffe weiter ausgeweitet werden, so dass nicht nur über Stunden, sondern über Tage und Wochen, Lieferketten beeinträchtigt werden, kann das gefährlich sein.“ Dazu müssten die Angriffe auf mehrere Teilsysteme gleichzeitig erfolgen – ein Szenario, welches bisher zwar nicht der Fall war, das aber gerade bei Angriffen durch staatliche Akteure ein durchaus realistisches Risiko bergen kann. Dem DZSF zufolge kommen Cyber-Angriffe auf das Schutzziel Integrität und damit auf die funktionale Sicherheit bisher in der Praxis in Deutschland nicht vor. „Ein klassisches Beispiel für einen Angriff auf die Integrität wäre die Manipulation von Signalen und Zugbeeinflussung“, erläutert Iffländer. Im schlimmsten Fall käme es dabei zu einer Kollision mit anschließender Entgleisung. Bisher bräuchten solche Angriffe jedoch ein erhebliches Spezialwissen in der Domäne und könnten – wenn überhaupt – nur unter immensem Ressourceneinsatz realisiert werden. Daher ist mit solcher Art von Attacken nach Einschätzung des Experten kurzfristig nicht zu rechnen.

## CYBER RESILIENCE: DIGITALE WIDERSTANDSFÄHIGKEIT DER SYSTEME ERHÖHEN

Sowohl die Verfügbarkeit als auch die Integrität der Bahninfrastruktur sieht sich aufgrund der Digitalisierung mit neuen Sicherheitsherausforderungen konfrontiert. Die digitale Überwachung und Steuerung von Infrastrukturen und Prozessen geht Hand in Hand mit einer fortschreitenden, dezentralen Vernetzung, auch im Ökosystem Schiene. Dazu erläutert Iffländer: „Immer mehr Systeme sind direkt oder indirekt mit dem Internet verbunden. Damit stellen sie attraktive Ziele dar, die teilweise mit Standard Hacking-Werkzeugen attackiert werden können." Das bisher eindrucksvollste Beispiel für eine derartige Attacke lieferte der groß angelegte Cyber-Angriff durch das Schadprogramm „Wanna Cry". Im Zuge des nun beinahe sechs Jahre zurückliegenden digitalen Sabotageakts wurden über 230 000 Windows-Rechner infiziert und weitreichender wirtschaftlicher Schaden verursacht. Auch die Bahn blieb von den Auswirkungen nicht verschont: Schwarze Anzeigentafeln, tote Videokameras und ausgefallene Ticketautomaten waren die Folgen der Attacke. Durch derartige Vorgänge rückt das Thema Cyber Resilience, also die Widerstandskraft der IT gegen Cyber-Angriffe, auch für das System Schiene immer mehr in den Fokus. In diesem Zusammenhang fordern IT-Sicherheitsexperten, kritische Infrastrukturen (KRITIS) wie die Schiene künftig stärker vor Cyber-Attacken zu schützen. Laut Frank Fischer, Chief Information Security Officer (CISO) bei der Deutschen Bahn AG (DB), braucht es Rahmenbedingungen, „die eine engere interdisziplinäre und organisationsübergreifende Zusammenarbeit zwischen Industrie und Behörden auf nationaler und europäischer Ebene vereinfachen." Wie Fischer gegenüber der Journalistin Julia Mutzbauer äußerte, benötigen wir in Deutschland „internationale und übergreifende Lage-Informationen, auch industrieübergreifend und entlang von Lieferketten, sowie Rahmenbedingungen, die eine noch engere Vernetzung mit Behörden und Nachrichtendiensten schaffen, um über ein Real-time-Lagebild die Verteidigung noch reaktionsschneller zu organisieren."

## SICHERHEITSLÜCKEN SIND OFT „TRIVIAL"

Neben der Verfügbarkeit und Integrität von Infrastruktur und operativen Prozessen ist der Schutz von sensiblen und personenbezogenen Daten ein weiterer zentraler Aspekt durchdachter Sicherheitsstrategien. Dass es keine großen Schadprogramme braucht, um eine Bresche in bestehende Sicherheitssysteme zu schlagen, zeigt die Aktion eines Sicherheitsforschers unter dem Pseudonym Flüpke: Der IT-Experte hackte sich im Sommer 2022 in die DB-Lounge der ersten Klasse ein. Er manipulierte dazu den Aztec-Code, der standardmäßig auf den Fahrkarten hinterlegt ist. Durch den Vergleich von Tickets der ersten und zweiten Klasse stellte er fest, dass der Code nur an wenigen Stellen durch andere Zeichen ersetzt werden musste. Laut Flüpke sei der Fehler der DB „trivial und absolut vermeidbar". Was die Bahn unfreiwillig erkennen durfte, gibt die Schweizerische Bundesbahnen AG (SBB) gezielt in Auftrag: Im Zuge des Bug-Bounty-Programms sind sogenannte ethische Hacker dazu aufgefordert, gezielt nach Möglichkeiten zum Klau von User-Daten und zur Datenmanipulation zu suchen. Die Belohnung: Bis zu 4000 EUR für eine aufgedeckte Lücke. Dazu ließ die Pressestelle des Schweizer Eisenbahnunternehmens verlautbaren: „Die SBB investiert schon länger jährlich einen

**EINIGE HANDLUNGSEMPFEHLUNGEN DER AKTUELLEN DZSF-STUDIE**

- Standards zur Cybersecurity wie NIST-CSF für bestimmte Standardanwendungen, zum Beispiel die EBA-Checklisten
- Prozesse zur Umsetzung der Richtlinien
- Sicherstellung von Support und Updates von Software schon im Vergabeprozess
- Stärkung des Bewusstseins für Cybersecurity beim Personal und auf den Managementebenen
- Steigerung der Branchenattraktivität für IT-Fachkräfte und insbesondere Cybersecurity-Spezialisten
- Offene branchenweite Austauschplattform zum Thema Cybersecurity schaffen
- Bedarf für kleinere und mittlere Unternehmen an einer Einmalförderung zur zielorientierten Einführung von Cybersecurity-Maßnahmen

***„Sollten solche Angriffe weiter ausgeweitet werden, so dass nicht nur über Stunden, sondern über Tage und Wochen, Lieferketten beeinträchtigt werden, kann das gefährlich sein.“***

Dr. Lukas Iffländer,
Referent Cybersecurity beim DZSF

zweistelligen Millionenbetrag in Cybersecurity und eine entsprechende Cyberstrategie wird konsequent umgesetzt.“

## BEDROHUNG DER PHYSISCHEN SICHERHEIT

Auch der Sabotageakt im Oktober 2022, bei dem in Norddeutschland für drei Stunden Fernzüge und Regionalbahnen ausfielen, ließ zuerst einen Cyber-Angriff vermuten. Wie sich jedoch bald herausstellen sollte, war der Grund für die weitreichende Kommunikationsstörung zwischen den Leitstellen physischer Natur: Saboteure hatten zielgerichtet Lichtwellenleiterkabel beschädigt. Ein Vorfall, der verdeutlicht, dass der Begriff der IT-Sicherheit in kritischen Infrastrukturen wie der Schiene über die gesamte Betriebstechnologie (Operational Technologie / OT) hinweg gedacht werden muss. Das Beratungshaus Gartner liefert eine anschauliche Definition: Demnach umfasst OT-Sicherheit „den Einsatz von Praktiken und Technologien, um (a) Personen, Anlagen und Informationen zu schützen, (b) physische Einrichtungen, Prozesse und Ereignisse zu beobachten und zu überwachen und (c) Statusänderungen bei Betriebstechnologie-Systemen von Unternehmen zu initiieren“. Dieser ganzheitliche Blick beschäftigt unter anderem auch die Innovationsinitiative Digitale Schiene Deutschland. Die Verantwortlichen legen „aufgrund der Komplexität der Systemarchitektur für das digitale Bahnsystem, dem angestrebten hohen Grad an Automatisierung und der Vielzahl an neu eingeführten Technologien wie Künstliche Intelligenz und Sensorik“ einen besonderen Fokus auf IT- / OT-Sicherheit.

## DZSF-BEFRAGUNG ZEIGT HANDLUNGSBEDARF AUF

Das DZSF hat im Zuge der Studie „Security und geplanter Technologieeinsatz“ die aktuellen Herausforderungen der Bahnbranche im Hinblick auf IT- und Cyber-Sicherheit identifiziert. Hierzu Cybersecurity-Referent Iffländer: „Besonders häufig wurde uns hierbei genannt, dass die Technik im Bahnsektor historisch gewachsen sei und oft Systeme im Einsatz sind, die auf alte Software-Versionen setzen und für die die Hersteller keine Updates mehr anbieten.“ Diese Systeme seien häufig unsicher, da Sicherheitslücken nicht behoben werden. Die Studie habe bei den EVU über alle Kategorien im Mittel einen Cybersecurity-Reifegrad von etwa 2 gezeigt. „Die Skala geht hierbei von 0 bis 5, wobei 0 das geringste Schutzniveau bedeutet und 5 das höchste, während ein ausreichendes Basisschutzniveau bei 3 erreicht ist“, so Iffländer. Interessant ist zudem, dass sich den Ergebnissen der DZSF-Studie zufolge viele Bahnunternehmen eine engere Führung durch Aufsichtsbehörden wie das BSI wünschen, während die aktuellen Normen wie etwa das KritisV oder die Fahrzeugnorm EN 50657 als zu pauschal empfunden werden.

***„Generell ist im Rahmen der Digitalisierung von Prozessen ein Bewusstsein für Security zu entwickeln.“***

Dr. Lukas Iffländer, Referent Cybersecurity beim DZSF

## IT-SICHERHEIT HAT UNTERNEHMENSKULTURELLE DIMENSION

Der Schutz von digitaler Infrastruktur ist nicht alleine eine Frage von Technologie und regulatorischen Vorgaben. Gegenüber dem DZSF haben viele Befragte angegeben, „dass im Unternehmen ein mangelndes Bewusstsein in Bezug auf Cybersecurity besteht, sowohl was die Mitarbeitenden als auch das Management angeht.“ Vielfach würde Technologie genutzt, die nicht ausreichend verstanden werde. „Wir haben diese Erkenntnis im Rahmen unserer Studie beim Thema Cloud-Dienste gemacht“, sagt Iffländer. So würden diese stark eingesetzt, obwohl viele Unternehmen ihren Wissensstand gegenüber Cloud-basierten Angeboten nur als mittel oder gering einschätzen und diese Dienste als hohen Risikofaktor betrachten. Dazu Iffländer: „Generell ist im Rahmen der Digitalisierung von Prozessen ein Bewusstsein für Security zu entwickeln.“ Neben einer Sensibilisierung für IT-sicherheitskritische Fragen fehlt es zudem schlicht an Expertise: Oftmals würden händeringend gesuchte IT-Fachkräfte in Bahnunternehmen schlechter bezahlt als in anderen Branchen, was die personellen Engpässe in diesem speziellen Fachgebiet weiter verschärft. Hier dürfen Bahnunternehmen im Sinne wehrhafter Sicherheitsstrategien künftig jedoch keine Kompromisse machen, wenn sie Angriffen auf ihre IT-Infrastrukturen weiterhin trotzen wollen. ═

Mit unserer Serie zur IT-Sicherheit auf der Schiene werfen wir einen detaillierten Blick auf die Herausforderungen und Kernfelder digitaler Security-Strategien. In den nächsten Ausgaben erwarten Sie Beiträge unter anderem zu folgenden Themen: „Cyber-Attacken auf die Bahn: Schutz gegen Hackerangriffe“, „DevSecOps spannt Bogen: Entwicklung, Betrieb und Sicherheit“ sowie „Internet-of-Railway-Things: OT-Security schützt Infrastruktur“.

### STUDIE BELEGT ERHÖHUNG DER IT-SICHERHEITS-BUDGETS

Laut einer Umfrage von Trend Micro, einem Anbieter von Cyber-Sicherheitslösungen, planen 63 % der befragten deutschen Unternehmen, 2023 mehr in ihre IT-Sicherheit zu investieren als in den Jahren davor. Zugleich zeigt die Studie kritische Verständnislücken auf. 45 % der deutschen Führungskräfte sehen in IT-Sicherheitsmaßnahmen eher ein notwendiges Übel als einen Business Enabler. Dieser Einschätzung setzt Richard Werner, Business Consultant bei Trend Micro, entgegen: „Unsere Studie zeigt, dass Cybersecurity ein entscheidender Faktor ist, wenn es darum geht, neue Kunden und Mitarbeiter zu gewinnen.“ In einer Zeit, in der jeder Euro zähle, sei es beunruhigend zu sehen, dass sich das Klischee von IT-Sicherheit als „Verhinderer“ selbst auf höchster Ebene hartnäckig hält.